TESIS PM-147501

MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PROYEK PERUSAHAAN XYZ MELALUI KOMBINASI COBIT, PMBOK, DAN ISO 31000

HURIN IIN
9114205320

DOSEN PEMBIMBING
Dr. Ir. Aris Tjahyanto, M.Kom

DEPARTEMEN MANAJEMEN TEKNOLOGI
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI
FAKULTAS BISNIS DAN MANAJEMEN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2017

LEMBAR PENGESAHAN

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar
Magister Manajemen Teknologi (M.MT)
di
Institut Teknologi Sepuluh Nopember
oleh :
Hurin Iin
NRP. 9114205320

Tanggal Ujian : 7 Juli 2017
Periode Wisuda : September 2017

Disetujui oleh:

1. **Dr. Ir. Aris Tjahyanto, M.kom** **(Pembimbing)**
   NIP: 196503101991021001

2. **Dr. Ir. R.V. Hari Ginardi, M.Sc.** **(Penguji)**
   NIP: 196505181992031003

3. **Faizal Mahananto, S.Kom, M.Eng, Ph.D** **(Penguji)**
   NIP: 5200201301010

Dekan Fakultas Bisnis dan Manajemen Teknologi,

Prof. Dr. Ir. Udisubakti Ciptomulyono, M.Eng.Sc
NIP. 19590318 198701 1 001

halaman ini sengaja dikosongkan

MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PROYEK PERUSAHAAN XYZ MELALUI KOMBINASI COBIT, PMBOK, DAN ISO 31000

Nama Mahasiswa : Hurin Iin
NRP : 9114205320
Pembimbing : Dr. Ir. Aris Tjahyanto, M.Kom

ABSTRAK

Perusahaan XYZ merupakan perusahan yang bergerak di bidang jasa konstruksi dan bangunan dengan spesialisasi pekerjaan pemasangan Aluminium Composite Panel. Pada saat pelaksanaan proyek, perusahaan XYZ sering menemui kendala/permasalahan. Salah satunya pada unit kerja IT misalnya desain tidak memiliki keterangan yang lengkap, revisi desain berkali-kali, file desain tidak terbaca pada komputer, hingga kesalahan dalam menghitung kebutuhan material. Kendala tersebut tentu memakan waktu pengerjaan proyek dan menyebabkan kerugian bagi perusahaan dan juga pemilik proyek.

Berdasarkan permasalahan di atas dibuatlah panduan untuk manajemen risiko teknologi informasi melalui kombinasi PMBOK, COBIT 5 *for Risk*, dan ISO 31000 dengan pertimbangan PMBOK memiliki keunggulan dalam menginisiasi setiap fase dalam proyek, COBIT unggul pada detail proses teknologi informasi, dan ISO 31000 sendiri merupakan standar internasional yang khusus digunakan dalam manajemen risiko.

Dari penelitian ini, melalui kombinasi PMBOK, COBIT 5 *for Risk*, dan ISO 31000 dihasilkan suatu panduan manajemen risiko teknologi informasi untuk mendukung proses pengerjaan proyek dan diperoleh 24 macam risiko yang berhasil diidentifikasi level risikonya. Penelitian ini juga menunjukkan bahwa 50% responden setuju bahwa panduan manajemen risiko teknologi informasi yang dihasilkan mudah dipahami dan diterapkan.

Kata kunci: COBIT 5 *for Risk*, ISO 31000, Manajemen risiko teknologi informasi, PMBOK.

halaman ini sengaja dikosongkan

INFORMATION TECHNOLOGY RISK MANAGEMENT IN XYZ COMPANY'S PROJECT USING COMBINATION OF COBIT, PMBOK, AND ISO 31000

By *: Hurin Iin*
NRP *: 9114205320*
Supervisor *: Dr. Ir. Aris Tjahyanto, M.Kom*

ABSTRACT

XYZ Company works in building construction which has specialty at Aluminium Composite Panel installation. This company encountered hazards as the project starts. Before the project get starting, the hazards comes from IT (Information Technology) team such as, the drawingshop has lack of information, continuous redesign of drawingshop, the files was unreadable, and error in calculate material requirement. These constraints certainly time consuming and cause loss for the project, either the company and project owner.

Based on that, a guideline for information technology risk management through the combination of PMBOK, COBIT 5 for Risk and ISO 31000 with consideration of PMBOK has an advantage in initiating each phase of the project, COBIT excels at the details on process of information technology, and ISO 31000 itself is an international standard which is specifically used in risk management.

This research obtained an information technology risk management guideline through the combination of PMBOK, COBIT 5 for Risk, and ISO 31000. Amount of 24 risks were identified with their level. The study also shows that 50% of respondents agree that the information technology risk management guidance obtained is easy to understand and apply.

Keyword: Information technology risk management, COBIT 5 for Risk, PMBOK, ISO 31000

halaman ini sengaja dikosongkan

KATA PENGANTAR

Dengan memanjatkan puji syukur Kehadirat Allah SWT atas segala karunia-Nya yang telah diberikan sehingga penulis dapat menyelesaikan tesis yang berjudul “Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ melalui Kombinasi COBIT, PMBOK, dan ISO 31000”.

Dengan ini, penulis menyampaikan penghormatan dan terima kasih kepada pihak-pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun tidak langsung, antara lain kepada:

1. Bapak Dr. Ir. Aris Tjahjanto, M.Kom selaku dosen pembimbing Tesis yang telah meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, petunjuk dan pengarahan dalam penyusunan proposal ini.
2. Direksi dan seluruh rekan kerja, khususnya unit IT yang telah membantu dan memberi banyak masukan pada penelitian ini.
3. Kedua orang tua saya yang telah memberikan semangat untuk menyelesaikan studi magister saya.
4. Sahabat terbaik saya yang setiap hari selalu melecut saya agar mengerjakan tesis setiap harinya, Fidi Wincoko Putro, S.ST, M.Kom.
5. Sahabat-sahabat mahasiswa MMT-ITS angkatan 2014 yang senantiasa saling memberikan dukungan kepada penulis.
6. Seluruh pihak yang telah banyak membantu yang tidak dapat disebutkan satu persatu dalam penyusunan proposal ini.

Penulis berharap semoga penelitian ini dapat bermanfaat dan dapat digunakan bagi pihak-pihak yang membutuhkan.

Surabaya, Juli 2017

Hurin Iin

halaman ini sengaja dikosongkan

DAFTAR ISI

DAFTAR TABEL

halaman ini sengaja dikosongkan

DAFTAR GAMBAR

halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perusahaan XYZ adalah perusahaan yang bergerak di bidang jasa konstruksi dan bangunan dengan spesialisasi pekerjaan pemasangan Aluminium Composite Panel (ACP) atau disebut juga aplikator Aluminium Composite Panel. Sejak didirikan pada tahun 2014, perusahaan yang memiliki 30 orang karyawan ini telah menangani ratusan proyek pemasangan ACP mulai dari hotel, showroom, SPBU, kantor, hingga apartemen.

Pekerjaan pemasangan ACP termasuk pekerjaan *finishing* bangunan. Pekerjaan ini biasanya dilakukan di fase terakhir sebuah proyek konstruksi. Yang harus dipersiapkan sebelum pekerjaan dimulai adalah survei lapangan dan melakukan pengukuran untuk membuat *shop drawing* (gambar) lengkap yang meliputi gambar denah, lokasi, bentuk, dan ukuran, serta perhitungan struktur seluruh komponen dan perkuatannya. Pekerjaan tersebut merupakan fase awal yang melibatkan banyak proses yang berkaitan dengan IT (desain dan informasi). Untuk proses selanjutnya biasanya pemilik proyek akan meminta membuat contoh jadi (*mock up*) untuk semua detail sambungan dan profil alumunium composite panel yang akan dipasang. ACP yang terpasang harus betul-betul akurat baik dalam level (*waterpass*) nya, ke-vertikalannya (unting-unting), sudut-sudutnya dan bidang datarnya. Tujuannya tentu agar ACP terpasang dengan kuat dan tidak mudah lepas nantinya. Setelah gambar selesai dibuat maka bisa dilakukan persiapan material dan alat yang dibutuhkan di lapangan agar bisa segera dilakukan pemasangan ACP.

Dalam proses pengerjaan proyek, perusahaan XYZ sering menemui kendala yang bisa menghambat proses pelaksanaan pekerjaan. Kendala di lapangan yang ditemukan adalah ACP yang dipasang melengkung karena rangkanya kurang kuat, ada kesalahan pada pemotongan modul ACP, pekerja yang kurang disiplin selama di lapangan, dan lain sebagainya. Di dalam tim IT paling sering ditemui kendala yang bisa menghambat pelaksanaan proyek seperti,

desain/gambar yang diserahkan tidak memiliki keterangan yang lengkap, revisi desain berkali-kali, file desain tidak terbaca pada komputer, hingga kesalahan dalam menghitung kebutuhan material. Kendala yang terdapat pada wilayah TI (teknologi informasi) ini sangat menghambat proses pelaksanaan proyek. Kesalahan tersebut dapat mengakibatkan jumlah material pada proyek di lapangan tidak mencukupi kebutuhan. Contoh lain seperti file desain/gambar mengalami kerusakan, datanya *corrupt* tidak bisa dibuka. Kendala ini bisa disebabkan karena *disk* atau media penyimpanan data telah terinfeksi virus. Atau bisa juga disebabkan karena proses penyimpanan yang tidak sempurna sehingga data menjadi *corrupt*. Akibatnya pada proyek tentu saja akhirnya menyebabkan penundaan terlaksananya pekerjaan di lapangan karena untuk menanganinya hal tersebut akan menyita waktu yang tidak sedikit. Kendala lain akan dijelaskan lebih detail pada bab II sub pembahasan Siklus Kegiatan Proyek Perusahaan XYZ.

Permasalahan yang berkaitan dengan TI seperti penjelasan di atas tentu memerlukan upaya dan penanganan agar tidak mengganggu pelaksanaan proyek. Oleh karena itu dibutuhkan manajemen risiko teknologi informasi agar perusahan tidak banyak dirugikan oleh keberadaan risiko tersebut. Perusahaan XYZ membutuhkan pannduan manajemen risiko yang mudah dipahami dan mudah diterapkan untuk mencegah dan mengurangi potensi terjadinya risiko serupa pada proyek-proyek yang sedang berjalan.

Pada penelitian ini, acuan yang dipakai untuk menyusun panduan manajemen risiko teknologi informasi adalah COBIT (*Control Objective for Information Technology and Related Technology*), PMBOK (*Project Management Body of Knowledge*), dan ISO (*International Standard Organisation*) 31000. COBIT digunakan untuk mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengatur keselarasan TI dengan bisnis. Dalam penelitian ini COBIT 5 *for Risk* sengaja dipilih untuk digunakan karena lebih spesifik membahas mengenai manajemen risiko teknologi informasi.

Karena COBIT hanya memberikan panduan kendali dan tidak memberikan panduan implementasi operasional, maka acuan yang dipakai disini akan dilengkapi oleh PMBOK dan ISO 31000. PMBOK adalah standar yang

banyak dipakai dalam manajemen proyek dan telah banyak diterapkan di banyak perusahaan karena kemudahannya untuk diaplikasikan. Melalui PMBOK bisa dilihat tahapan proses untuk keseluruhan proyek. Diharapkan melalui PMBOK bisa dilihat lebih jelas risiko yang ada pada setiap fase proyek.

ISO 31000 telah banyak digunakan oleh perusahaan-perusahaan dalam mengelola risiko karena di dalamnya terkandung prinsip-prinsip untuk mewujudkan manajemen risiko yang efektif dan tata kelola risiko yang baik. Keberadaan prinsip manajemen risiko, penetapan konteks eksternal, dan pemisahan antara kerangka kerja dengan proses manajemen risiko menjadi keunggulan kompetitif yang dimiliki oleh ISO 31000. Keunggulan inilah yang akan dimanfaatkan untuk mendukung *framework* yang telah disebutkan sebelumnya untuk manajemen risiko teknologi informasi pada perusahaan XYZ.

Berdasar keunggulan masing-masing *framework* diatas, diharapkan penggunaan ketiganya akan menciptakan kombinasi yang tepat dalam pembuatan panduan manajemen teknologi informasi untuk perusahaan XYZ. Dari hasil kombinasi *framework* gabungan tersebut juga diharapkan bisa mendukung keseluruhan proses pada saat pelaksanaan proyek melalui upaya pengendalian risiko TI beserta dampaknya. Demikianlah alasan penggunaan ketiga *framework* (COBIT 5 *for Risk*, PMBOK, dan ISO 31000) tersebut di atas.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana membuat panduan manajemen risiko teknologi informasi pada proyek yang cocok diterapkan di perusahaan XYZ melalui kombinasi COBIT 5 *for Risk*, PMBOK, dan ISO 31000?
2. Bagaimana hasil evaluasi kemudahan penggunaan panduan pada saat panduan manajemen risiko teknologi informasi yang dihasilkan tersebut diterapkan di perusahaan XYZ?

1.3 Tujuan dan manfaat penelitian

Tujuan dari penelitian ini adalah mengusulkan panduan manajemen risiko teknologi informasi pada proyek bagi perusahaan XYZ melalui kombinasi *framework* COBIT 5 *for Risk*, PMBOK, dan ISO 31000 dan mengevaluasi hasilnya apakah mudah dipahami dan diterapkan oleh perusahaan XYZ.

Manfaat dari penelitian ini diharapkan dapat membantu mempercepat pelaksanaan proyek bagi perusahaan XYZ melalui pengelolaan risiko teknologi informasi.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

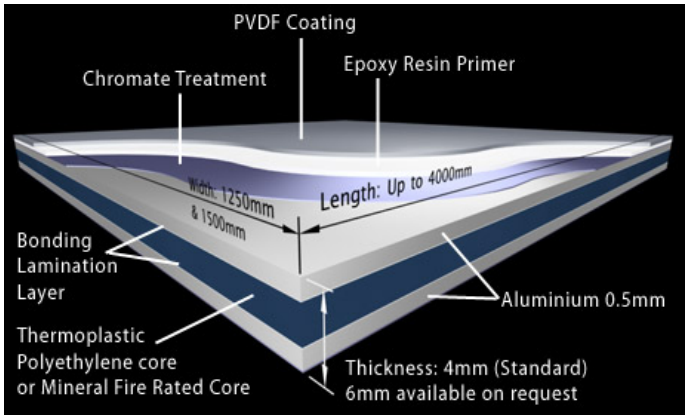
1. Penelitian difokuskan pada pengelolaan risiko teknologi informasi pada proyek di perusahaan XYZ.
2. Hal yang diteliti tidak meliputi wilayah keuangan akuntansi perusahaan XYZ. Perusahaan XYZ dianggap memiliki kondisi keuangan yang sehat.

BAB 2
KAJIAN PUSTAKA DAN DASAR TEORI

2.1 Perusahaan XYZ

Perusahaan XYZ adalah perusahaan yang bergerak di bidang jasa konstruksi dan bangunan dengan spesialisasi pekerjaan pemasangan Aluminium Composite Panel (ACP). Perusahaan ini didirikan di Surabaya pada awal tahun 2014 dengan personil awal sebanyak 15 orang. Hingga saat ini jumlah pegawainya terus berkembang dan mencapai 30 orang. Jumlah pekerjaan pemasangan ACP yang pernah ditangani oleh perusahaan XYZ terbilang cukup banyak. Sudah ratusan proyek yang pernah menggunakan jasa perusahaan XYZ untuk pekerjaan pemasangan ACP. Mulai dari skala kecil hingga skala besar, lokasi pekerjaan telah tersebar di beberapa kota di Indonesia, terutama Surabaya dan sekitarnya. Gedung atau bangunan yang dikerjakan antara lain hotel, restoran, kantor, apartemen, showroom, SPBU, dan minimarket.

Aluminium Composite Panel atau biasa disingkat ACP merupakan material berbahan aluminium yang fungsinya dipakai sebagai pelapis dinding bangunan menggantikan cat atau keramik. Kelebihannya dibandingkan dengan cat dan keramik dinding adalah warnanya tidak mudah pudar serta tahan terhadap suhu panas dan jamur. Struktur lapisan ACP ditunjukkan pada Gambar 2.1 berikut ini.



Gambar 2.1 Struktur lapisan Aluminium Composite Panel

Dalam pelaksanaan proyeknya perusahaan XYZ memiliki empat proses / fase yaitu, fase survei dan desain, fase kontrak, fase pengerjaan, dan fase serah terima. Untuk mencegah terjadinya risiko buruk pada proyek maka sejak awal proses harus selalu dilakukan pengecekan dengan teliti apakah urutan prosedur yang dijalankan sudah benar atau belum.

Sebagai contoh, pada fase survei dan desain harus dipastikan bahwa desain gambar sudah memiliki keterangan yang lengkap. Desain modul ACP juga harus dibuat seefisien mungkin agar *waste* (sisa material) yang dihasilkan minimal. Proses menghitung kebutuhan material ACP juga harus penuh ketelitian agar tidak timbul kesalahan dalam membuat *Bill of Quantity* (BoQ). Pada fase kontrak jangan sampai ada kesalahan tulisan dalam pembuatan kontrak. Pada fase pengerjaan jangan sampai ada kesalahan pemotongan modul, pemasangan rangka, maupun kesalahan lainnya. Hal ini tentu dimaksudkan agar pada saat fase serah terima pekerjaan perusahaan XYZ mendapat nilai positif dari klien.

Dari bahasan di atas dapat diketahui bahwa pencegahan dan penanganan risiko di perusahaan XYZ dinilai cukup penting keberadaannya. Namun, sayang manajemen risiko di Perusahaan XYZ belum berjalan dengan baik. Hal ini terlihat dari munculnya masalah-masalah kecil di proyek seperti kesalahan perhitungan kebutuhan material, *waste* yang besar, konstruksi rangka yang tidak sempurna, ACP lepas dari rangka, sulitnya mengontrol kinerja tukang/pekerja proyek, dan lain sebagainya. Dimana kesemuanya tadi bisa mempengaruhi keberhasilan dan keterlambatan waktu penyelesaian proyek.

Untuk mengetahui berapa lama waktu yang dibutuhkan untuk pekerjaan pemasangan ACP. Data yang menunjukkan volume pekerjaan yang pernah dikerjakan oleh perusahaan XYZ beserta rata-rata lama pengerjaannya ditunjukkan pada Tabel 2.1 di bawah ini.

Tabel 2.1 Proyek yang pernah dikerjakan Perusahaan XYZ

No	**NamaProyek**	**Volume Pekerjaan (m^2)**	**Lama Pengerjaan (hari)**	**Rata-rata vol pekerjaan/hari (m^2/hari)**
1	Spindo	1418	97	14,6
2	Jeep Showroom	128,74	14	9,2

3	Citi9 Lamongan	443,65	16	27,7
4	Citi9 Balongbendo	359,82	12	29,9
5	IAIN Tulungagung	2285,12	39	58,6
6	Aria Hotel	1102	30	36,3
7	Gerbang Tol Sadang	1103,49	43	25,7
8	Pelabuhan Tanjung Tembaga	392,986	12	32,7
9	Legundi Gudang	1468,39	56	26,5
10	Pemkab Bojonegoro	2300	157	14,6
11	Power House Nilam	370	16	23,1
12	Ruko Yondi	296,14	31	9,6

Sumber: Dokumen Perusahaan XYZ, 2016

Dari Tabel 2.1 di atas dapat diketahui bahwa rata-rata volume pekerjaan per hari jumlahnya berbeda-beda antar proyek. Faktor yang mempengaruhinya bermacam-macam. Untuk faktor yang berkaitan dengan teknologi informasi terdapat paling banyak pada fase-fase awal proyek atau sebelum pengerjaan seperti yang telah disebutkan pada paragraf sebelumnya. Mengenai detilnya akan dijelaskan pada sub bab berikutnya.

2.2 Proyek

Dalam kegiatan sehari hari kita sering kali menyebutkan proyek sebagai suatu pengerjaan suatu kegiatan namun dalam buku *A Guide to the Project Management Body of Knowledge* (PMBOK) disebutkan bahwa proyek adalah pekerjaan temporer yang dikerjakan untuk menciptakan suatu produk atau pelayanan yang memiliki keunikan.

Proyek disebut unik karena produk atau layanan yang dihasilkan nantinya memiliki kekhususan tersendiri dibandingkan dengan yang lain. Jadi proyek pada dasarnya adalah suatu kegiatan melaksanakan pekerjaan yang sifatnya temporer untuk menghasilkan produk yang khas.

2.2.1 Siklus Kegiatan Proyek (*Project Life Cycle*)

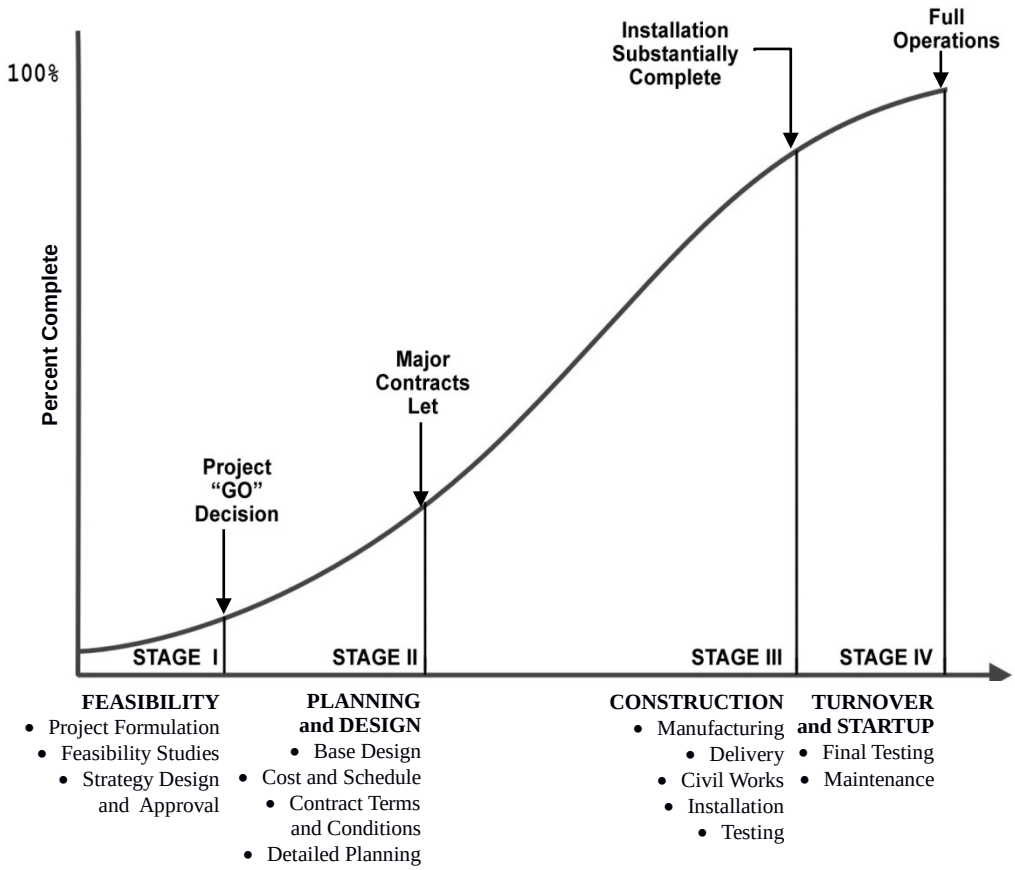
Karena sifat pekerjaan yang temporer, setiap proyek selalu memiliki siklus yang disebut sebagai siklus kegiatan proyek (*Project Life Cycle*). Siklus ini berlangsung mulai dari pra proyek hingga pasca proyek. Secara umum siklus ini

memiliki fase yang tipikal untuk segala macam proyek yaitu fase awal, fase tengah dan fase akhir. Yang membedakan siklus proyek satu dengan yang lain adalah detail pelaksanaan proyek itu sendiri.

Siklus kegiatan proyek ini digunakan untuk menjabarkan tahap mulainya proyek hingga tahap selesainya proyek dan secara umum menjelaskan tentang pekerjaan teknis apa yang harus dilakukan pada tiap fase dan siapa yang seharusnya terlibat pada tiap fase.

Deskripsi kegiatan dalam fase-fase proyek bisa sangat sederhana sampai sangat detil. Namun karakteristik umum yang biasanya ada dalam deskripsi kegiatan pada tiap fase proyek adalah (a) biaya dan jumlah pekerja umumnya sedikit pada awal kegiatan dan terus meningkat hingga akhir kegiatan, dan kemudian menukik tajam seiring selesainya proyek tersebut; (b) pada awalnya persentase kemungkinan menyelesaikan proyek berada pada titik terendah karena pada tahap awal ini segala kemungkinan yang dapat menghambat berjalannya proyek banyak dan mungkin terjadi. Sedangkan tingkat risiko dan ketidakpastian berada pada titik yang paling tinggi pada awal proyek karena pada risiko dan ketidakpastian akan terus bermunculan seiring berjalannya proyek. Kemungkinan keberhasilan proyek meningkat seiring dengan progress pelaksanaan proyek; (c) Kemampuan pemegang saham untuk mempengaruhi hasil akhir dari proyek sangat tinggi pada awal proyek dan kemudian menurun seiring berjalannya proyek. Penyebab hal ini biasanya adalah biaya terhadap perubahan dan koreksi terhadap kesalahan yang berkembang seiring berjalannya proyek.

Mengutip pendapat Morris dalam buku PMBOK, siklus hidup proyek konstruksi adalah seperti yang digambarkan pada Gambar 2.2 dibawah ini.



Gambar 2.2 Siklus Kegiatan Proyek (Konstruksi) Morris (*PMBOK 2000)*

Tahap I adalah Tahap *Feasibility* dimana suatu proyek direncanakan kemudian diadakan studi kelayakan serta mematangkan strategi desain dan mendapatkan persetujuan dari yang berwenang. Layak tidaknya suatu proyek akan ditentukan pada tahap ini.

Tahap II adalah Tahap Desain dan Perencanaan dimana desain dasar, biaya dan penjadwalan, dokumen kontrak kerja dan perencanaan yang lebih mendetail dibuat.

Tahap III adalah Tahap Konstruksi dimana pada tahap ini bahan-bahan untuk proyek dibuat, diantarkan ke lokasi, dikerjakan oleh kontraktor, instalasi jaringan dan pengetesan. Pada akhir tahap ini fasilitas yang dikerjakan sudah harus selesai dan dapat dipergunakan dengan baik.

Tahap IV adalah Tahap Serah Terima dan pengoperasian dimana pada tahap ini dilakukan tes akhir dan pemeliharaan. Pada tahap ini fasilitas yang

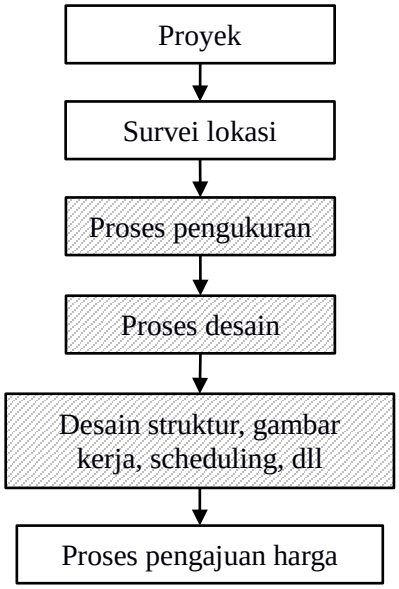
dibangun sudah dioperasikan secara penuh.

2.2.2 Siklus Kegiatan Proyek Perusahaan XYZ

Dibawah ini akan dijelaskan fase-fase dalam siklus kegiatan proyek pemasangan ACP di perusahaan XYZ yang memiliki empat fase yaitu fase survei dan desain, fase kontrak, fase pengerjaan dan fase serah terima.

2.2.2.1 Fase Survei dan Desain

Pada tahap ini yang pertama dilakukan adalah survei lokasi proyek yang meliputi area gedung dan sekitarnya, serta kondisi dari gedung yang akan dipasang ACP. Adapun proses-proses yang dilakukan pada fase ini ditunjukkan pada Gambar 2.3 berikut:



Gambar 2.3 Fase Survei dan Desain pada Siklus Proyek Perusahaan XYZ

Pada Gambar 2.3 diatas yang diarsir mengandung banyak kegiatan/aktivitas yang berkaitan dengan TI. Sedangkan yang tidak diarsir mengandung sedikit kegiatan/aktivitas yang berkaitan dengan TI. Urutan langkah fase diatas adalah sebagai berikut, perusahaan melakukan survei lokasi seperti pengecekan area dan sekitar lokasi, mengecek konstruksi bangunan apakah sudah selesai dan siap untuk dipasang rangka ACP. Setelah itu proses tersebut berlanjut

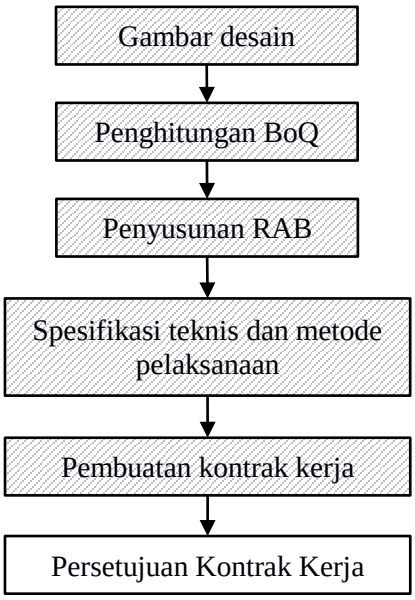
ke pengukuran bagian bangunan yang hendak dipasang ACP. Pada bagian ini aktivitas TI yang dilakukan adalah menyalin data ukuran ke dalam komputer. Risiko TI yang mungkin terjadi adalah kesalahan input angka pengukuran pada komputer. Kesalahan ini terlihat sepele namun akibatnya bisa fatal karena bisa berakibat pada desain bangunan yang dibuat tidak sesuai dengan ukuran sebenarnya. Risiko ini bisa merembet pada risiko lain di proses selanjutnya.

Dari proses pengukuran dilanjutkan ke proses desain yang di dalamnya meliputi desain bangunan dan modul ACP, gambar kerja, perkiraan harga, penjadwalan proyek, dan sebagainya. Kesemuanya merupakan aktivitas yang banyak melibatkan TI. Untuk membuat desain gambar digunakan *software* Autocad. Sedangkan untuk pembuatan jadwal proyek menggunakan *software* proyek dari Microsoft. Risiko TI yang terjadi pada proses ini antara lain berupa proses desain yang lambat dan memakan waktu lama karena adanya revisi dari pemilik proyek. Terkadang desain modul ACP yang dibuat harus dirombak total karena permintaan klien sehingga harus dilakukan penyesuaian lagi terhadap ukuran modulnya. File desain yang dibuat juga bisa saja tiba-tiba rusak atau *corrupt* dan tidak bisa dibuka. Risiko lainnya adalah komputer yang dipakai tiba-tiba mengalami kemacetan dan mati pada saat mendesain dan menyusun jadwal proyek. Jika semua itu terjadi maka perusahaan akan sangat dirugikan sekali.

Selanjutnya proses pengajuan atau penawaran harga kepada klien. Proses ini masih melibatkan TI karena menggunakan *software* teks editor dari Microsoft. Risiko TI yang terjadi adalah lupa mengupdate harga pada saat kurs dolar berubah. Dikarenakan harga dasar material sifatnya sangat fluktuatif mengikuti nilai kurs dolar. Sehingga membutuhkan update terus-menerus.

2.2.2.2 Fase Kontrak

Pada proyek ini, terjadi proses persetujuan kontrak yang tahapannya akan dijelaskan pada Gambar 2.4 dibawah ini:



Gambar 2.4 Fase Kontrak pada Siklus Proyek Perusahaan XYZ

Pada Gambar 2.4 diatas dijelaskan bahwa untuk membuat kontrak perusahaan akan mencetak gambar desain. Setelah itu dilanjutkan dengan menghitung BoQ (*Bill of Quantity*) atau jumlah kebutuhan bahan material. Jumlah ini dapat diketahui dengan menghitung volume satuan pekerjaan terlebih dahulu. Proses perhitungannya dilakukan menggunakan bantuan *software Ms. Excel* dari Microsoft. Risiko TI yang ada pada proses ini adalah kesalahan hitung bisa menyebabkan jumlah material yang distok kurang atau berlebih. Untuk itu perhitungan dituntut harus teliti supaya hasilnya benar.

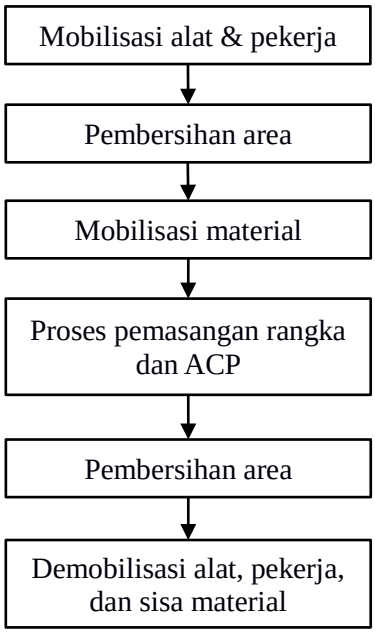
Proses selanjutnya adalah penyusunan RAB (Rencana Anggaran Belanja), yaitu perhitungan banyaknya anggaran biaya suatu bangunan dan upah, serta biaya-biaya lain yang berhubungan dengan pelaksanaan proyek. Pembuatannya biasanya menggunakan *software* hitung dari Microsoft. Risiko TI yang ada pada proses ini adalah kesalahan input harga yang bisa mengakibatkan RAB yang dihasilkan juga salah.

Proses selanjutnya adalah pembuatan spesifikasi teknis dan metode pelaksanaan proyek. Wujudnya adalah berupa penyerahan dokumen teknis material dan penyerahan contoh material untuk memastikan material yang dipakai memenuhi syarat. Risiko TI yang mungkin muncul pada proses ini dan proses

selanjutnya adalah terkadang karena pengiriman dokumen teknis melalui email dan sangat bergantung pada kondisi server apakah email tersebut berhasil terkirim atau gagal. Proses berikutnya adalah menyusun dokumen kontrak kerja. Setelah klien menerima dan membaca kontrak kerja tersebut, maka bisa dilakukan penandatanganan persetujuan kontrak kerja. Jika terdapat pasal yang membuat klien merasa keberatan maka bisa dilakukan negosiasi terhadap pasal tersebut berdasar kesepakatan bersama sebelum dilakukan penandatangan kontrak.

2.2.2.3 Fase Pengerjaan

Setelah fase kontrak maka tahap selanjutnya adalah fase pengerjaan. Prosesnya dijelaskan pada Gambar 2.5 berikut ini:



Gambar 2.5 Fase Pengerjaan pada Siklus Proyek Perusahaan XYZ

Pada tahap awal proses fase pengerjaan, hal yang dilakukan adalah mobilisasi alat dan pekerja yaitu mendatangkan peralatan kerja seperti scaffolding, gondola, mesin potong dan pekerja yang diperlukan dalam proyek ini. Fase selanjutnya adalah pembersihan area lokasi. Pada fase ini lokasi proyek dibersihkan dari barang/benda yang dapat mengganggu proses pemasangan ACP. Proses ini dilakukan untuk menghindari terjadinya kecelakaan kerja.

Setelah area dibersihkan serta dianggap sudah dapat digunakan untuk menumpuk dan menyimpan material yang dibutuhkan, maka proses mobilisasi material dapat dilakukan. Proses ini dilakukan bertahap sampai proyek selesai, karena tidak mungkin mendatangkan seluruh material ke lokasi pada tahap awal proyek karena keterbatasan tempat. Setelah material yang dibutuhkan sampai ke lokasi proyek maka tahap selanjutnya adalah tahap pemasangan rangka ACP. Dimana pada tahap ini material berupa rangka dipasang terlebih dahulu sebagai pondasi untuk memasang ACP. setelah rangka terpasang, barulah ACP dapat dipasang.

Ketika proses pengerjaan sudah selesai dikerjakan, maka selanjutnya dilakukan pembersihan area proyek lagi. Hal ini dimaksudkan supaya bangunan dan lokasi bersih dari segala sampah dan sisa material sehingga klien bisa langsung menggunakannya. Proses selanjutnya setelah pembersihan area selesai dilakukan adalah demobilisasi alat dan peralatan proyek dari lokasi proyek. Pada tahap ini semua peralatan yang digunakan tadi dikeluarkan dari lokasi proyek.

Pada fase ini tidak banyak aktivitas yang terkait dengan teknologi informasi. Risiko TI yang muncul mungkin berupa kesalahan laporan progres proyek yang disimpan dalam bentuk file.

2.2.2.4 Fase Serah Terima

Fase serah terima dilakukan ketika fase konstruksi sudah selesai dilakukan. Biasanya fase ini dilakukan dalam beberapa tahapan. Serah terima I dilakukan setelah fase pengerjaan selesai dilakukan, serah terima II dilakukan setelah masa pemeliharaan selesai. Fase ini juga sedikit melibatkan teknologi informasi sehingga risiko yang berkaitan dengan TI yang mungkin muncul adalah tidak melakukan update data pada proyek yang sudah selesai.

2.3 Manajemen Risiko

Penerapan manajemen risiko tidak hanya untuk proyek-proyek bangunan saja namun juga pada hal-hal lain seperti keuangan perusahaan, perbankan, proses industri dan masih banyak hal lainnya.

Dalam konteks proyek, risiko adalah suatu kondisi atau peristiwa tidak pasti yang jika terjadi mempunyai efek positif atau negatif terhadap sasaran proyek. Sebuah risiko mempunyai penyebab dan jika risiko itu terjadi, akan ada konsekuensi. Jika yang terjadi adalah peristiwa yang tidak pasti, maka dampaknya adalah pada biaya, jadwal, dan kualitas proyek.

Ada 4 hal utama dalam mengkategorikan sebuah risiko, yaitu adanya (a) ketidakpastian (*uncertainty*) ketiadaan informasi yang diperlukan yang membuat sebuah risiko tidak dapat diprediksi (b) peristiwa (*events*) jika mengkategorikan penambahan biaya atau keterlambatan sebagai risiko adalah keliru karena hal tersebut bukan peristiwa melainkan dampak atau konsekuensi dari risiko peristiwa (c) masa depan (*future*) kejadian masa lampau bukanlah sebuah risiko tetapi problem aktual dan krisis yang perlu penyelesaian kembali adalah risiko. Ciri manajemen risiko adalah proaktif dan selalu melihat ke depan, berbeda dengan manajemen krisis yang berciri reaktif dan melihat ke belakang. (d) keuntungan dan tujuan (*interest and objectives*).

Jika peristiwa yang potensial terjadi di masa depan tidak mempengaruhi tujuan suatu organisasi, maka peristiwa yang berpotensi terjadi tersebut bukanlah sebuah risiko bagi organisasi tersebut.

Dalam manajemen proyek, manajemen risiko adalah sebuah proses sistematis yang bertujuan untuk mengidentifikasi dan mengatur risiko, menangani risiko (menghindari, mengurangi, mengalihkan, atau menerima), melalui penerapan sistem dan prosedural.

Dalam manajemen risiko diperlukan beberapa tipe pengambilan keputusan. Tabel 2.2 dibawah ini adalah *Risk Assessment Matrix* yang digunakan sebagai *tool* untuk memberikan rating risiko dengan tingkat Sangat Tinggi (*Extreme*), Tinggi (*High*), Sedang (*Medium*), atau Rendah (*Low*) dengan membandingkan antara variabel probabilitas suatu peristiwa dengan dampaknya.

Tabel 2.2 *Risk Assessment Matrix*

Dampak (Konsekuensi)	Major	Medium	High	Extreme
	Moderate	Medium	Medium	High
	Minor	Low	Medium	Medium
		Kemungkinan (0 – 33%)	Kemungkinan (33% – 66%)	Kemungkinan (66% – 100%)
		Kemungkinan terjadinya risiko		

Tingkat atau level risiko Dampak rendah dengan kemungkinan rendah berarti risiko yang berada pada pojok kiri bawah merupakan risiko yang tingkat risikonya rendah, sehingga dapat diabaikan. Dampak rendah dengan kemungkinan tinggi, risiko yang berada pada pojok kanan bawah memiliki tingkat risiko sedang. Jika risiko ini terjadi, anda dapat dengan mudah mengatasinya dan meneruskan proyek. Tetapi, bagaimanapun harus mencari cara agar kemungkinan terjadinya risiko ini dapat ditekan.

Dampak tinggi dengan kemungkinan rendah, risiko tinggi memiliki dampak yang besar jika terjadi. Untuk mengantisipasi hal ini anda harus melakukan hal-hal yang dapat mengurangi dampak yang diakibatkan jika risiko ini terjadi serta memiliki rencana cadangan jika risiko ini tidak dapat diatasi.

Dampak tinggi dengan kemungkinan tinggi, risiko yang berada pada pojok kanan atas ini merupakan risiko yang harus paling diwaspadai. Risiko ini merupakan prioritas utama yang harus ditangani. Biasanya untuk menanggulangi risiko ini digunakan sistem manajemen risiko dimana didalamnya terdapat proses identifikasi, analisis dan pengendalian kejadian / peristiwa.

2.4 Manajemen Risiko Teknologi Informasi

Saat ini teknologi informasi (TI) memainkan peran penting dalam banyak bisnis. Jika saat ini TI merupakan bagian terpenting pengelolaan bisnis, maka sangat penting untuk mengidentifikasi risiko untuk sistem TI dan data yang dikelola dalam sistem TI, kemudian berupaya untuk mengurangi atau mengelola risiko tersebut, dan untuk mengembangkan rencana penanganan ketika risiko telah teridentifikasi yang dapat terjadi di dalam sistem dan data yang dikelola dalam

sistem TI.

Menurut Rahmadhanty (2010), manajemen risiko teknologi Informasi (TI) adalah kemampuan organisasi dalam mengurangi risiko-risiko TI yang mungkin akan menghambat pencapaian tujuan organisasi terkait dengan pemanfaatan TI itu sendiri. Teknologi informasi juga bisa membawa risiko. Seringkali dalam melakukan bisnis dalam skala global, sistem dan jaringan telah menjadi terlalu mahal bagi semua perusahaan untuk ditangani. Di beberapa industri, teknologi informasi merupakan sumber daya kompetitif untuk melakukan diferensiasi dan memberikan keunggulan kompetitif sedangkan di perusahaan lainnya teknologi informasi membantu dalam mempertahankan hidup perusahaan.

Di dalam Jurnal *Internasional De La Salle University volume 13* (Flores et al. 2011) membahas mengenai kekuatan, kelemahan perusahaan, dan bagaimana teknologi informasi dapat mendukung proses bisnis. Serta bagaimana perusahaan dapat melacak posisi teknologi informasinya dan meningkat ke level berikutnya. Penelitian mengenai pentingnya mengelola manajemen risiko yang dilakukan oleh *(Parent & Reich,* 2009), (*Enslin*, 2012) membahas apa saja risiko-risiko yang dapat ditimbulkan jika teknologi informasi tidak dapat dikelola dengan benar. Menurut *Enslin* salah satu masalah yang dapat ditimbulkan adalah penggunaan data atau penyalahgunaan data bisa mengakibatkan kesalahan dalam mengambil keputusan.

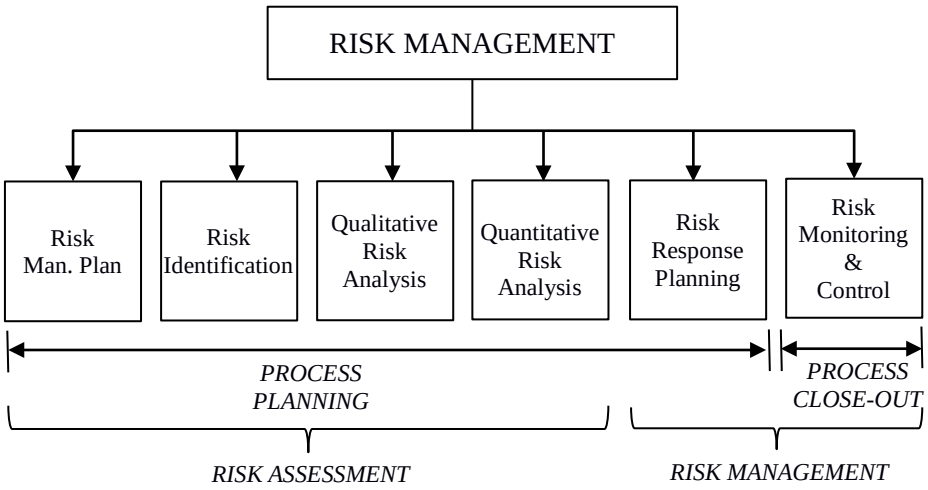
2.5 Project Management Body of Knowledge (PMBOK)

Definisi manajemen risiko menurut PMBOK, yaitu sebagai berikut:

a) Merupakan proses formal, dimana faktor-faktor risiko secara sistematis diidentifikasi, dianalisis dan ditangani.
b) Merupakan suatu metode pengelolaan sistematis yang formal yang berkonsentrasi pada mengidentifikasi dan mengendalikan area atau kejadian-kejadian yang berpotensi untuk menyebabkan terjadinya perubahan yang tidak diinginkan.

c) Di dalam konteks suatu proyek, merupakan suatu seni dan ilmu pengetahuan dalam mengidentifikasi, menganalisis dan merespon terhadap faktor-faktor risiko yang ada selama pelaksanaan suatu proyek.

PMBOK ini memiliki tingkat kedetailan yang tinggi dan disertai penjelasan tekniknya. Kelebihan inilah yang akan diunggulkan pada penelitian ini. Di dalam buku PMBOK edisi ke-5 disebutkan Manajemen Risiko meliputi proses melakukan perencanaan manajemen risiko, identifikasi, analisis kualitatif, analisis kuantitatif, perencanaan respon, dan pengendalian risiko pada proyek seperti ditunjukkan pada Gambar 2.6 di bawah ini.



Gambar 2.6 Manajemen Risiko (PMBOK *Fifth Edition*, 2013)

Pada Gambar 2.6 diatas, terdapat enam proses dalam manajemen risiko menurut PMBOK. Penjelasannya adalah sebagai berikut:

1. Perencanaan Manajemen Risiko

   Perencanaan yang hati-hati dan jelas akan menentukan kesuksesan lima proses manajemen risiko lainnya. Tahap ini merupakan proses untuk menentukan langkah-langkah dalam menyelesaikan risiko yang timbul dalam suatu proyek. Proses perencanaan ini penting dalam menentukan tingkat, tipe, dan kelayakan manajemen risiko apakah setara dengan risiko serta pentingnya proyek terhadap organisasi, untuk menyediakan sumber daya yang cukup, serta

waktu untuk aktivitas manajemen risiko serta untuk menguatkan dasar pada persetujuan untuk mengevaluasi risiko. Input dalam proses ini antara lain adalah faktor lingkungan perusahaan, asset dalam proses organisasi, lingkup kerja proyek serta rencana manajemen proyek. Adapun teknik yang digunakan dalam merencanakan menajemen risiko adalah dengan rapat perencanaan dan analisis.

Pada rapat ini nantinya dibahas rencana dasar untuk menghadapi risiko. Biaya untuk mengatasi risiko, serta jadwal aktivitas akan dikembangkan untuk dijadikan jadwal dan anggaran proyek. Tanggung jawab risiko akan disepakati pada tahap ini.

Perencanaan manajemen risiko menjabarkan bagaimana manajemen risiko akan disusun dan diterapkan dalam proyek dimana didalamnya terdapat metode manajemen risiko, peraturan dan tanggung jawab masing masing personel, anggaran manajemen risiko, format laporan serta pemilihan waktu yang mendefinisikan kapan dan seberapa sering proses manajemen risiko akan dilakukan seiring siklus proyek.

Risk Breakdown Structure (RBS) juga termasuk dalam perencanaan ini dimana RBS ini nantinya akan ditinjau kembali pada tahap indentifikasi risiko. Definisi kemungkinan terjadinya risiko dan dampaknya pada tahap awal juga dijabarkan pada tahap ini, dalam hal ini untuk mendefinisikan kualitas dan kredibilitas analisis risiko secara kualitatif akan membutuhkan tingkat kemungkinan serta dampak risiko. Skala relatif yang menggambarkan nilai probabilitas dari “sangat disukai “ sampai “hampir dipastikan” dapat dipakai. Sebagai alternatif dapat digunakan angka probabilitas pada skala umum (misal 0.1, 0.2, 0.3, dst). Matriks probabilitas dan dampak juga dapat dihasilkan pada proses ini. Tabel ini juga dapat dikembangkan sebagai tabel definisi kesempatan (*opportunity*) dengan cara yang sama. *Tracking* nantinya digunakan untuk semua aktivitas yang dianggap berisiko untuk digunakan demi kepentingan proyek saat ini maupun proyek lain selain itu juga sebagai bahan pembelajaran. Dokumen ini sangat diperlukan dalam proses audit.

2. Identifikasi Risiko

   Adalah proses menentukan bagaimana suatu risiko dapat mempengaruhi proyek serta mendokumentasikan ciri-ciri tiap risiko supaya setiap risko dapat tercatat dan terdokumentasi dengan baik dan tim proyek dapat mengantisipasi setiap risiko yang terjadi. Proses pengidentifikasian perlu dilakukan berulang kali agar definisinya jelas dan mudah untuk dimengerti dan dianalisa.

3. Analisis Risiko Kualitatif

   Adalah proses memprioritaskan risiko untuk analisis dan tindakan lebih lanjut dengan menilai dan menggabungkan probabilitas kejadian serta dampak dari risiko yang ada. Analisis ini biasanya dapat dilakukan dengan cepat dan murah, berguna untuk menyusun prioritas dalam perencanaan penanggulangan risiko, serta menjadi dasar untuk analisis secara kuantitatif jika diperlukan Adapun yang menjadi dasar untuk menganalisis secara kualitatif antara lain adalah (a) data proyek terdahulu dimana dari data tersebut dapat dipelajari apa saja yang menjadi risiko dari proyek tersebut; (b) lingkup pekerjaan yang jelas akan membantu mengetahui apa saja yang akan dilakukan untuk menyelesaikan proyek tersebut sehingga risiko yang dihadapi juga jelas; (c) rencana manajemen risiko dimana didalamnya terdapat peraturan serta tanggung jawab masing-masing personel yang terlibat dalam proyek; (d) daftar risiko yang telah dibuat pada tahap identifikasi risiko.

   Teknik yang bisa dipakai untuk analisis kualitatif adalah dengan membuat penilaian kemungkinan terjadinya risiko beserta dampak yang dapat ditimbulkan. Tingkat kemungkinan beserta dampak ini dapat diperoleh melalui wawancara atau rapat dengan tim TI.

4. Analisis Risiko Kuantitatif

   Adalah proses numerik untuk menganalisa pengaruh dari risiko yang telah diidentifikasi sebelumnya terhadap nilai obyektif proyek secara keseluruhan. Tujuannya agar diperoleh keterangan nilai risiko untuk mendukung proses pengambilan keputusan dalam rangka mengurangi angka ketidakpastian pada proyek. Metode analisis ini biasanya dilakukan berdasarkan prioritas risiko yang dihasilkan dari analisis kualitatif. Analisis kuantitatif biasanya harus diulang kembali setelah perencanaan

penanggulangan risiko sebagai bagian dari monitoring dan kontrol terhadap risiko.

Teknik yang bisa dipakai untuk analisis kuantitatif antara lain, mengumpulkan data kejadian sebelumnya, membuat pemodelan distribusi, pemodelan simulasi, hingga penilaian oleh para ahli.

5. Perencanaan Penanganan Risiko

Perencanaan pengendalian risiko merupakan proses dari pengembangan pilihan serta penentuan tindakan yang paling efektif sehingga diharapkan dapat meningkatkan kesempatan dan mengurangi risiko yang dipandang dari sisi negatif yaitu tantangan.

Secara umum ada empat tipe pengendalian risiko yaitu pengabaian/pengurangan risiko (*risk avoidance/reduction*), transfer risiko (*risk transfer*), mitigasi risiko, dan penerimaan risiko (*risk acceptance*), sedangkan untuk risiko yang dipandang dari sisi positif dalam hal ini adalah kesempatan, maka strategi yang diterapkan adalah dengan mengeksploitasi, membagi dan meningkatkannya (*enhance*). Ada kalanya strategi penerimaan dijalankan terhadap risiko yang disadari nantinya akan timbul ketika proyek berjalan. Hal ini dilakukan karena memang tidak semua risiko dapat dikurangi ataupun dihindari.

6. Pemantauan dan Pengendalian Risiko

Pengawasan dan kontrol risiko merupakan proses dari pengidentifikasian, analisis dan perencanaan terhadap risiko yang baru timbul, mengawasi terjadi atau tidaknya risiko yang ada dalam daftar, menganalisa kembali risiko yang sudah ada dalam daftar, memonitor kondisi yang tiba-tiba terjadi serta membuat rencana penyelesaiannya, memonitor risiko yang tersisa, dan meninjau ulang pelaksanaan rencana penanggulangan risiko serta mengevaluasi keefektifannya. Adapun metode yang umum dipakai dalam tahap ini adalah *risk reassessment, risk audits, variance and trend analysis, technical performance measurement, reserve analysis* dan *status meetings.*

PMBOK membagi siklus hidup proyek ke dalam 5 fase yaitu inisiasi (*initiation*), perencanaan (*planning*), pelaksanaan (*execution*), pengawasan dan

pengendalian (*monitoring and controlling*), serta penutupan (*closing*). Dari pembahasan sebelumnya mengenai siklus hidup proyek perusahaan dan siklus hidup proyek menurut PMBOK, didapati bahwa risiko TI yang diteliti pada kasus ini menurut PMBOK masuk pada fase awal proyek yaitu Fase Perencanaan.

Fase Perencanaan dalam PMBOK mencakup sembilan area pengetahuan (*knowledge area*) yang memiliki tujuan sebagai panduan dalam pelaksanaan proyek. Salah satu area pengetahuan tersebut adalah manajemen risiko (*risk management*).

2.6 COBIT 5 *for Risk*

Control Objective for Information & Related Technology (COBIT) adalah sekumpulan dokumentasi *best practice* untuk *IT Governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI (Sasongko, 2009).

COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengatur keselarasan TI dengan bisnis. Selain itu, kerangka kerja juga memastikan bahwa TI memungkinkan bisnis, memaksimalkan keuntungan, resiko TI dikelola secara tepat, dan sumber daya TI digunakan secara bertanggung jawab (Tanuwijaya dan Sarno, 2010).

COBIT diperkenalkan sebagai *framework* untuk tata kelola dan manajemen TI yang didesain menjadi satu kesatuan *framework* yang digunakan untuk tata kelola sekaligus manajemen TI. COBIT 5 *for Risk* mendefinisikan risiko TI sebagai risiko bisnis. Risiko TI merupakan peristiwa-peristiwa yang ada kaitannya dengan TI yang berpotensi mengakibatkan kegagalan atau kerugian pada bisnis. Dalam COBIT, risiko tidak harus selalu dihindari karena tidak ada bisnis yang tidak mengandung risiko. Oleh karena itu dalam bisnis, perusahaan perlu untuk menentukan *risk appetite* (tingkat risiko yang akan diambil, yaitu merupakan tingkat dan jenis risiko yang bersedia diambil oleh perusahaan dalam rangka mencapai sasaran perusahaan).

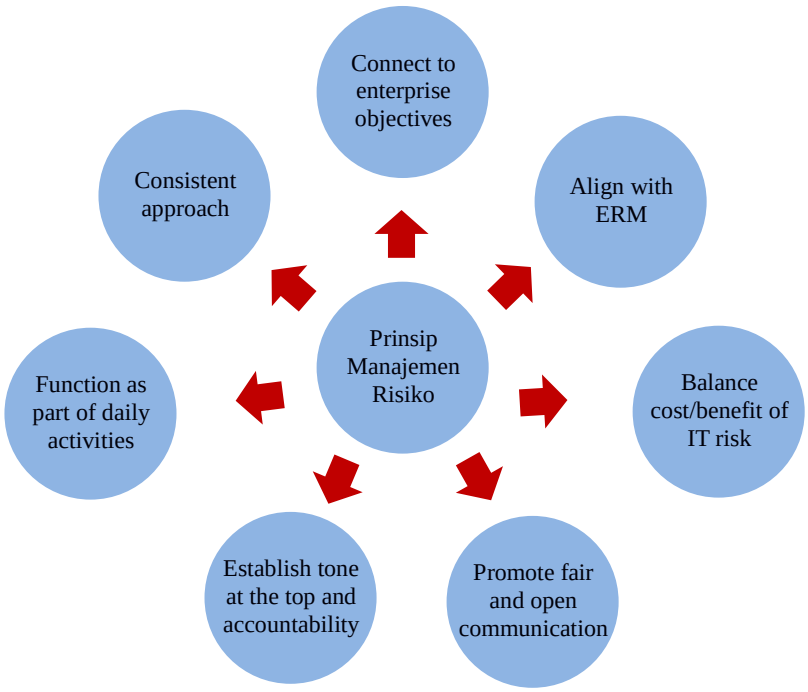
Risiko-risiko yang ada tentu harus dikelola, bukan dihindari. Dalam dunia bisnis kesediaan mengambil risiko adalah hal yang mutlak. Inilah

pentingnya *risk appetite*, yaitu untuk menetapkan nilai maksimum terhadap risiko mengenai berapa banyak proposisi bisnis yang di dalamnya menganduk risiko TI yang akan diambil untuk mencapai nilai proposisi dalam mewujudkan tujuan perusahaan.

COBIT 5 *for Risk* memiliki 7 *enabler* (penggerak) yaitu:

[1] Prinsip, Kebijakan, dan Kerangka kerja

Prinsip, kebijakan, dan kerangka kerja adalah alat untuk mengkomunikasikan aturan perusahaan dalam mendukung *governance objectivity* dan nilai perusahaan. Dengan adanya kebijakan, maka prinsip-prinsip yang dibuat bisa dijalankan dan keputusan-keputusan yang diambil akan selaras dengan prinsip tersebut. Terdapat 7 (tujuh) prinsip manajemen risiko pada COBIT 5 *for Risk* seperti ditunjukkan pada Gambar 2.7 berikut ini.

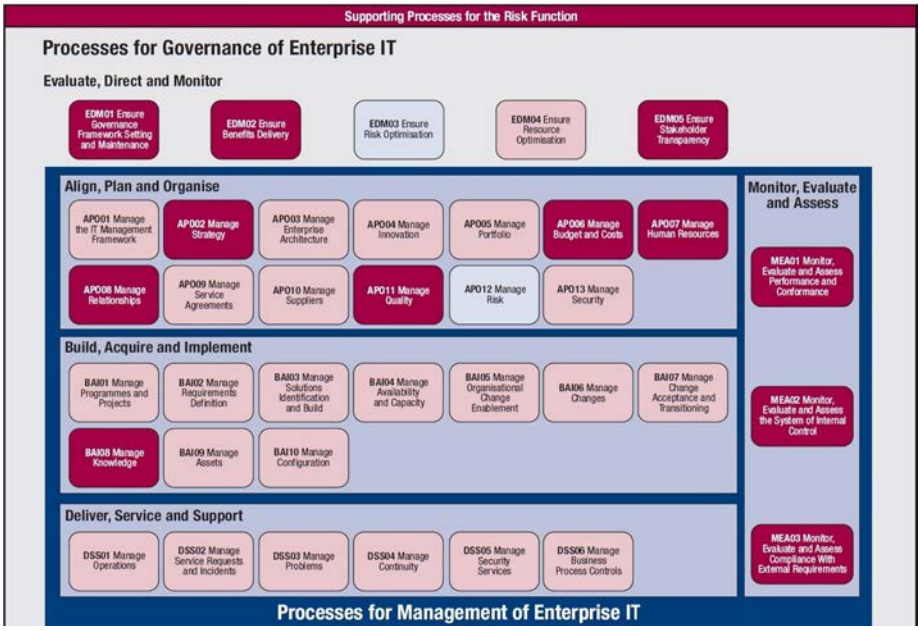


Gambar 2.7 Prinsip Manajemen Risiko pada COBIT 5 *for Risk*

[2] Proses

Terdapat proses kunci pendukung manajemen risiko dan proses lain (bukan kunci) yang juga mendukung pelaksanaan manajemen risiko seperti

ditunjukkan pada Gambar 2.8. Proses pendukung kunci ditandai warna merah gelap, pendukung lainnya ditandai warna merah muda. Proses kunci atau proses inti sendiri diwarnai biru muda.



Gambar 2.8 Proses pendukung Manajemen Risiko COBIT

[3] Struktur Organisasi

Susunan organisasi dibagi menjadi inti dan pembantu dimana keduanya memiliki tingkat kewenangan yang berbeda dalam mengakses dan menangani risiko.

[4] Budaya, Etika, dan Perilaku

Pola komunikasi dalam perusahaan, budaya perusahaan, dan aturan-aturan agar mendukung fungsi risiko.

[5] Informasi

Tujuannya adalah mendapatkan informasi yang berkualitas, akurat, dan lengkap. Contohnya adalah laporan daftar risiko, *risk scenario*, rencana penanganan risiko, faktor penyebab risiko, dan laporan kerugian yang diakibatkan risiko.

[6] Layanan, Infrastruktur, dan Aplikasi

Infrakstruktur, aplikasi, dan layanan harus mampu mendukung proses manajemen risiko.

[7] Manusia, Keahlian, dan Daya saing

Sumber daya manusia yang dimiliki perusahaan harus ada yang mempunyai keahlian dan berdaya saing dalam menganalisa dan mengelola risiko.

COBIT 5 *for Risk* menerapkan 5 prinsip COBIT dalam pengaturan risiko yaitu:

[1] Memenuhi kebutuhan pemangku kepentingan

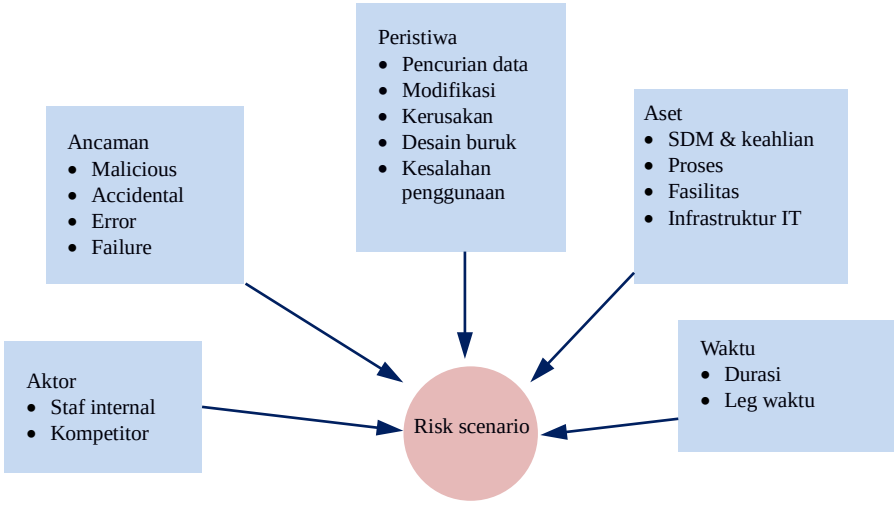
[2] *Covering enterprise end-to-end*

[3] Menerapkan kesatuan kerangka kerja yang terintegrasi

[4] Menerapkan pendekatan menyeluruh

[5] Memisahkan *governance* dari manajemen

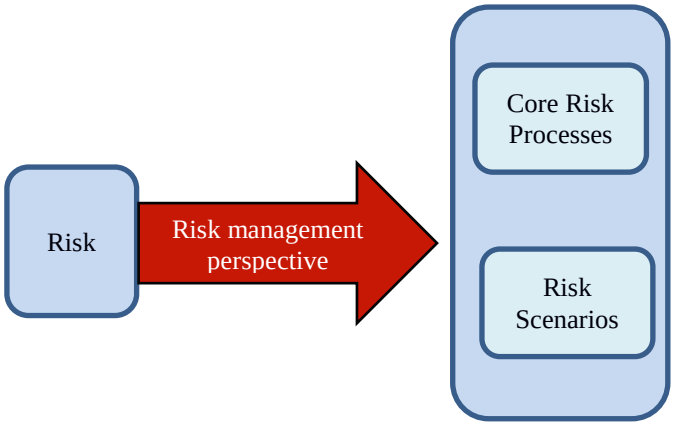
Dalam COBIT, risiko-risiko direpresentasikan dalam komponen manajemen risiko yang nama nya *risk scenario* yang informasinya diperlukan untuk mengidentifikasi, analisis dan penanganan risiko. *Risk scenario* adalah representasi keberadaan dari sebuah risiko beserta penilaiannya.



Gambar 2.9 *Risk scenario* (COBIT 5 *for Risk* ISACA, 2013)

Risk scenario adalah elemen kunci di dalam proses manajemen risiko pada COBIT. Gambar 2.9 di atas menunjukkan elemen-elemen dari *risk scenario*.

Risk scenario nantinya akan dijadikan input untuk proses analisis risiko. Sedangkan proses untuk mengelola keberadaan suatu risiko dimasukkan ke dalam *core risk process*. Jadi di dalam COBIT representasi keberadaan risiko dan proses pengelolaannya disendiri-sendirikan seperti terlihat pada Gambar 2.10 di bawah ini:



Gambar 2.10 Pembagian risiko pada COBIT

Core Risk Process terdiri dari 2 domain yaitu, domain EDM03 dan APO12. Penjelasannya sebagai berikut:

1) EDM03 - *Ensure Risk Optimisation*

EDM03 merupakan bagian dari *risk governance*. Proses *Ensure Risk Optimisation* berfokus pada pengelolaan risiko dan toleransi risiko yang berhubungan dengan nilai TI pada perusahaan dan memastikan bahwa resiko TI perusahaan tidak melebihi kemampuan dan toleransi perusahaan dalam menerima resiko, serta mengidentifikasi dan mengelola dampak dari resiko TI terhadap nilai-nilai pada perusahaan, dan mengurangi terjadinya kegagalan.

Proses ini meliputi pemahaman, artikulasi dan komunikasi dari *risk appetite, risk tolerance,* dan identifikasi dari manajemen risiko terhadap nilai perusahaan yang berhubungan dengan TI beserta dampaknya.

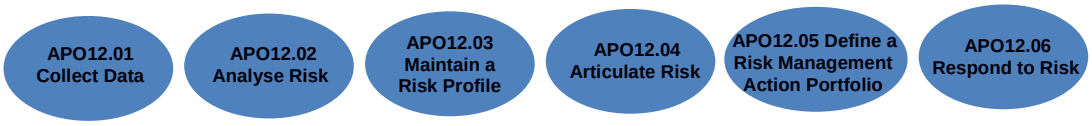
Tujuan dari proses ini adalah untuk:

1. Mendefinisikan dan menetapkan ambang batas resiko dan memastikan bahwa kunci risiko terkait TI diketahui.

2. Secara efektif dan efisien mengelola risiko perusahaan terkait *IT ciritical*.
3. Memastikan risiko TI yang terkait dengan perusahaan tidak melebihi *risk appetite.*

2) APO12 - *Manage Risk*

APO12 merupakan bagian dari *risk management* (manajemen risiko). Deskprisi dari proses APO12 adalah secara terus menerus mengidentifikasi, menilai dan mengurangi risiko yang berhubungan dengan TI didalam level toleransi yang ditentukan oleh manajemen perusahaan. Proses manajemen risiko ditunjukkan pada Gambar 2.11 berikut ini.



Gambar 2.11 Proses Manajemen Risiko (APO12)

Penjabaran APO12 dalam COBIT 5 *for Risk* adalah sebagai berikut:

1. Pengumpulan data (APO12.01)

   Mencari dan mengumpulkan data yang relevan untuk proses identifikasi, analisis, dan pelaporan mengenai risiko-risiko TI dan hal yang berkaitan dengannya secara efektif. Aktivitas yang terlibat pada proses ini antara lain menetapkan metode pengumpulan data, mendaftar data yang berperan penting dalam TI baik secara internal maupun eksternal, melakukan survey data sebelumnya beserta kerugian yang ditimbulkan, hingga memberi *highlight* pada data yang memiliki peran penting.
2. Analisis risiko (APO12.02)

   Mengembangkan informasi yang berguna dalam mendukung keputusan pengambilan risiko dengan memperhitungkan keterkaitannya terhadap faktor-faktor yang mempengaruhi risiko pada suatu bisnis.
3. Menyusun profil risiko (APO12.03)

   Menjaga inventarisasi risiko yang diketahui dan atribut risiko (termasuk frekuensi yang diharapkan, potensi dampak dan respon terhadap

risiko) serta sumber daya terkait, kemampuan dan kegiatan pengendalian arus.

4. Menjabarkan risiko (APO12.04)

   Memberikan informasi tentang keadaan saat kedapatan ada risiko dan peluang yang berkaitan dengan TI pada waktu yang tepat untuk semua pemangku kepentingan demi menentukan respon yang tepat.

5. Membuat portfolio kegiatan manajemen risiko (APO12.05)

   Mengelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima ke dalam bentuk sebuah portofolio.

6. Respon risiko (APO12.06)

   Merespon secara tepat waktu dengan langkah-langkah efektif untuk membatasi besarnya kerugian dari peristiwa risiko yang berkaitan dengan TI yang terjadi.

Faktor penyebab risiko dibagi menjadi 4 kategori yaitu, lingkungan internal, lingkungan eksternal, kemampuan mengelola risiko, dan kemampuan TI dari perusahaan.

Risk capacity adalah kerugian kumulatif yang bisa ditanggung oleh perusahaan tanpa mengorbankan hidup matinya perusahaan. Sedangkan *risk tolerance* adalah tingkat risiko yang bisa diterima oleh perusahaan. Dari COBIT bisa diketahui bahwa jika keberadaan *risk appetite* lebih rendah daripada *risk capacity*, atau dengan kata lain kemampuan perusahaan dalam mengatur risiko tidak melebihi batas kemampuan maksimal, maka perusahaan relatif berada di kondisi *sustainable* (dapat bertahan). Namun jika *risk appetite* ini tingginya melebihi *risk capacity*, maka kondisi perusahaan biasanya sulit untuk bertahan (*unsustainable*). Karena itu sebaiknya *risk appetite* diusahakan untuk tidak melebihi *risk capacity*.

Dalam penanganan risiko negatif pada COBIT 5 *for Risk* terdapat empat opsi yang bisa dipilih yaitu, pengabaian risiko (*avoid*), pencegahan risiko (*mitigate*), transfer risiko (*transfer/share*), dan penerimaan risiko (*accept*). Sedangkan untuk risiko positif juga terdapat empat opsi yaitu, mengusahakan (*exploit*), memperbesar kemungkinan (*enhance*), berbagi (*share*), dan

mengabaikan (*ignore*). Dalam setiap penanganan yang dilakukan harus dilakukan evaluasi sesuai dengan daur proses manajemen risiko. Pencegahan risiko juga perlu dilakukan untuk mengurangi probabilitas dari munculnya keberadaan suatu risiko. Sesuai dengan bunyi pepatah lama, bagaimanapun juga mencegah itu lebih baik daripada mengobati. Sehingga pencegahan ini penting dalam proses manajemen risiko.

COBIT menyediakan kerangka kerja komprehensif yang dapat membantu perusahaan untuk mencapai tujuannya dalam konteks tata kelola dan pengendalian TI pada perusahaan. COBIT mampu membuat TI menjadi lebih terkelola dan teratur dalam seluruh lini perusahaan. Bagusnya lagi, COBIT dapat digunakan untuk perusahaan berskala kecil maupun besar, baik itu perusahaan komersial, nirlaba, maupun sektor pelayanan publik.

COBIT 5 *for Risk* dibangun di atas *framework* COBIT 5 dengan berfokus pada risiko dan menyediakan penjelasan yang lebih rinci serta panduan praktis bagi para profesional maupun pihak lain yang berkepentingan di semua tingkat perusahaan. COBIT 5 *for Risk* menyajikan dua perspektif tentang bagaimana menggunakan COBIT dalam konteks risiko, yaitu fungsi risiko dan manajemen risiko.

Fungsi risiko berfokus pada apa yang dibutuhkan untuk membangun dan mempertahankan fungsi risiko dalam suatu perusahaan. Sedangkan manajemen risiko berfokus pada tata kelola dan manajemen proses risiko inti yaitu bagaimana mengoptimalkan risiko dan bagaimana mengidentifikasi, menganalisis, menanggapi dan melaporkan risiko setiap hari.

Dari buku COBIT 5 *for Risk* juga diketahui keselarasan COBIT 5 *for Risk* dengan *framework-framework* manajemen proses lainnya. Contohnya ISO 31000. Ternyata COBIT 5 *for Risk* mampu mengakomodasi prinsip, kerangka kerja, dan proses manajemen risiko yang dimiliki oleh ISO 31000.

2.7 ISO 31000

ISO 31000: 2009 *Risk Management – Principles and Guidelines* merupakan sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. Standar

internasional yang diterbitkan pada 13 November 2009 ini dapat digunakan oleh segala jenis organisasi dalam menghadapi berbagai risiko yang melekat pada aktivitas mereka. Definisi risiko menurut buku ISO 31000 yaitu, efek dari ketidakpastian terhadap pencapaian sasaran organisasi. Sehingga darinya didapat pengertian bahwa manajemen risiko adalah aktivitas-aktivitas terkoordinasi yang dilakukan dalam rangka mengelola dan mengontrol sebuah organisasi terkait dengan risiko yang dihadapinya.

ISO 31000 : 2009 *Risk Management – Principles and Guidelines* menentukan sebelas prinsip yang perlu dipahami dan diterapkan pada kerangka kerja dan proses manajemen risiko untuk memastikan efektivitasnya. Sebelas prinsip tersebut adalah:

1) Memberikan nilai tambah dan melindungi nilai organisasi

   Prinsip ini menyatakan bahwa kegiatan manajemen risiko harus dapat meningkatkan kapabilitas organisasi dalam menyerap risiko agar organisasi dapat memanfaatkan peluang-peluang yang ada sekarang dan dapat muncul di masa depan (memberikan nilai tambah bagi organisasi). Selain itu, manajemen risiko juga harus dapat mengantisipasi risiko-risiko berdampak buruk yang dapat membahayakan pencapaian sasaran organisasi (melindungi nilai organisasi).

2) Bagian terpadu dari seluruh proses organisasi

   Manajemen risiko harus melekat pada seluruh proses organisasi karena setiap proses organisasi menghadapi risiko yang dapat menyebabkan sasaran proses tersebut tidak tercapai. Prinsip ini juga secara implisit menyatakan bahwa manajemen risiko tidak hanya menjadi tanggung jawab top management dari organisasi, tetapi seluruh bagian dari organisasi.

3) Bagian dari pengambilan keputusan

   Setiap alternatif keputusan mengandung risiko tersendiri. Untuk itu dalam memilih alternatif keputusan, organisasi harus mempertimbangkan unsur risiko dari setiap alternatif, ketersediaan sumber daya organisasi, serta kapabilitas dan toleransi organisasi dalam menyerap risiko.

4) Secara khusus menangani ketidakpastian

Setiap organisasi tentu menghadapi ketidakpastian dalam perjalanannya mencapai sasaran mereka. Manajemen risiko membantu mengurangi aspek ketidakpastian dengan memberi ukuran (parameter) terhadap konsekuensi dari risiko. Parameter ini menunjukkan eksposur organisasi terhadap risiko tersebut, yang nantinya akan menentukan penanganan risiko. Penanganan risiko diharapkan dapat membantu organisasi mereduksi eksposur risiko dan ketidakpastian yang dihadapi organisasi.

5) Sistematis, terstruktur, dan tepat waktu

Prinsip ini menyatakan bahwa manajemen risiko harus dijalankan secara konsisten dan terintegrasi pada seluruh organisasi. Pembentukan *risk governance* yang memperjelas kewenangan, peran, dan tanggung jawab dari setiap unit organisasi berkaitan dengan manajemen risiko juga diperlukan untuk mendukung efektivitas manajemen risiko.

6) Berdasarkan informasi terbaik yang tersedia

Penerapan manajemen risiko harus didukung dengan informasi terbaik yang dapat diperoleh organisasi. Informasi terbaik terdiri dari tiga aspek, yaitu relevan, terpercaya, dan tepat waktu. Untuk mendukung perolehan informasi terbaik, organisasi dapat melakukan proses dokumentasi dan membentuk database informasi (misalnya membuat *risk register*). Tanpa adanya informasi terbaik, penerapan manajemen risiko dapat menjadi tidak tepat sasaran.

7) Disesuaikan dengan kebutuhan organisasi

Setiap individu, unit kerja, dan organisasi tentu memiliki karakteristik tersendiri dan menghadapi risiko yang berbeda-beda. Salah satu keunggulan dari ISO 31000: 2009 adalah menyediakan standar generik yang dapat diadaptasi sesuai dengan kebutuhan pemangku risiko dalam usaha mencapai tujuannya masing-masing. Untuk itu, setiap pemangku risiko tidak dapat hanya mengikuti sistem manajemen risiko yang dibentuk oleh unit atau organisasi lain, tapi harus menyesuaikan dengan keadaan dan risiko yang dihadapinya.

8) Mempertimbangkan faktor budaya dan manusia

Penerapan manajemen risiko harus mempertimbangkan kultur, persepsi, dan kapabilitas manusia, termasuk memperhitungkan perselisihan kepentingan antara organisasi dengan individu di dalamnya. Hal ini penting

untuk diperhatikan karena penerapan manajemen risiko dilakukan oleh sumber daya insani dari organisasi.

9) Transparan dan inklusif

Penerapan dan informasi mengenai manajemen risiko harus melibatkan seluruh bagian organisasi. Keberadaan suatu risiko juga tidak boleh disembunyikan atau dilebih-lebihkan.

10) Dinamis, berulang, dan responsif terhadap perubahan

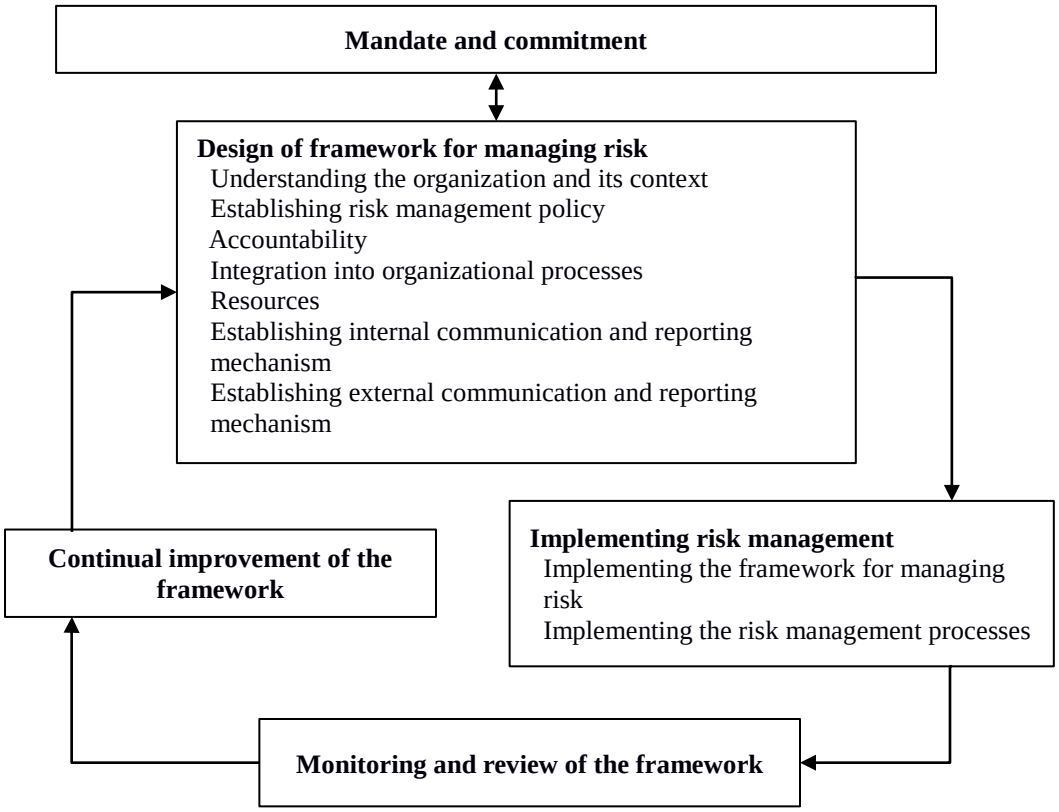
Prinsip ini menyatakan bahwa manajemen risiko harus diimplementasikan secara konsisten dan berulang, serta harus dapat dapat memfasilitasi perubahan pada sisi internal dan eksternal organisasi. Proses *monitoring* dan *review* menjadi aktivitas kunci dalam mendeteksi perubahan dan memfasilitasi penyesuaian pada manajemen risiko.

11) Memfasilitasi perbaikan sinambung dan peningkatan organisasi

Keberadaan manajemen risiko harus diperbaiki dari waktu ke waktu sesuai dengan perkembangan konteks internal dan eksternal organisasi. Perbaikan berkelanjutan ini diharapkan dapat membawa perbaikan yang signifikan pada organisasi.

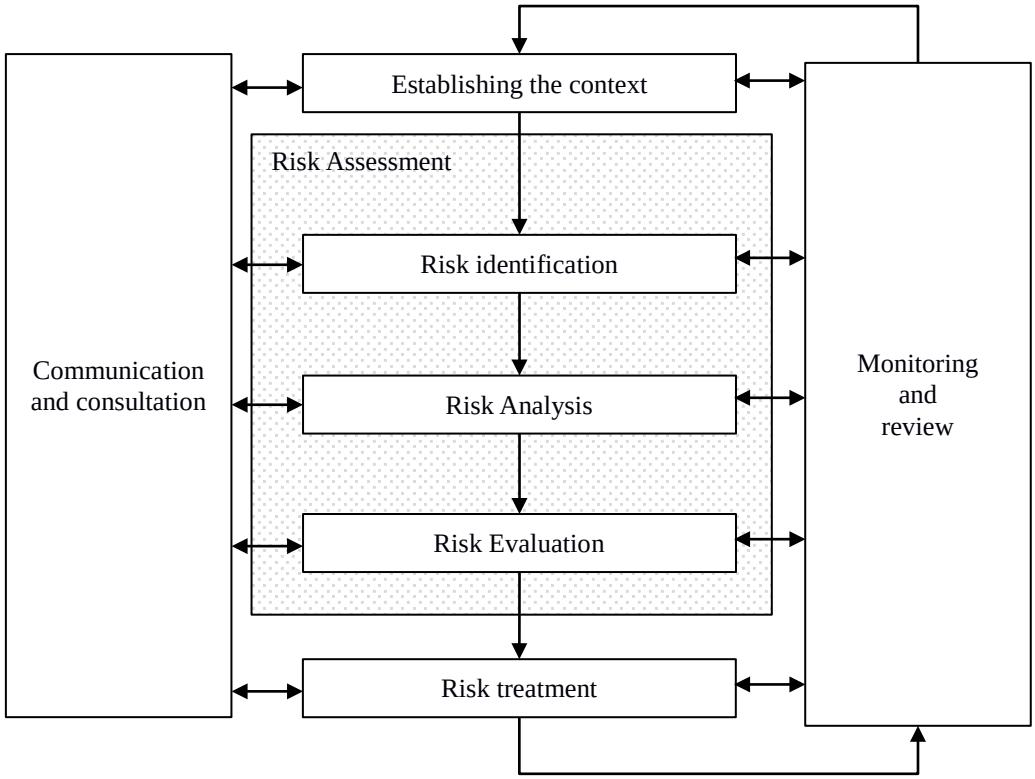
Menurut ISO, manajemen risiko suatu organisasi hanya dapat efektif bila mampu menganut prinsip-prinsip di atas tersebut. Agar dapat berhasil baik, manajemen risiko harus diletakkan dalam suatu kerangka manajemen risiko. Kerangka ini akan menjadi dasar dan penataan yang mencakup seluruh kegiatan manajemen risiko di segala tingkatan organisasi. Kerangka manajemen risiko ini disusun khas ISO yaitu berdasarkan siklus *Plan* (mendesain kerangka manajemen risiko), *Do* (mengimplementasikan kerangka manajemen risiko), *Check* (memonitor dan mereview kerangka manajemen risiko), dan *Act* (perbaikan terus menerus kerangka manajemen risiko), dengan sebelumnya harus mendapatkan mandat dan komitmen berlanjut dari manajemen organisasi.

Kerangka kerja ini akan membantu organisasi mengelola risiko secara efektif melalui penerapan proses manajemen risiko. ISO 31000 memiliki kerangka kerja seperti pada Gambar 2.12 di bawah ini:



Gambar 2.12 *Framework* ISO 31000

Perencanaan kerangka kerja manajemen risiko mencakup pemahaman mengenai organisasi dan konteksnya, menetapkan kebijakan manajemen risiko, menetapkan akuntabilitas manajemen risiko, mengintegrasikan manajemen risiko ke dalam proses bisnis organisasi, alokasi sumber daya manajemen risiko, dan menetapkan mekanisme komunikasi internal dan eksternal. Setelah melakukan perencanaan kerangka kerja, maka dilakukan penerapan proses manajemen risiko. Dalam penerapan manajemen risiko, perlu dilakukan monitoring dan review terhadap kerangka kerja manajemen risiko. Setelah itu, kerangka kerja manajemen risiko perlu diperbaiki secara berkelanjutan untuk memfasilitasi perubahan yang terjadi pada konteks internal dan eksternal organisasi. Proses-proses tersebut kemudian berulang kembali untuk memastikan adanya kerangka kerja manajemen risiko yang mengalami perbaikan berkesinambungan dan dapat menghasilkan penerapan manajemen risiko yang andal.



Gambar 2.13 Proses Manajemen Risiko ISO 31000

Dalam ISO 31000 Proses manajemen risiko dibagi menjadi lima proses seperti ditunjukkan pada Gambar 2.13 di atas, yaitu:

1) Penetapan konteks (*establishing the context*)

Penetapan konteks bertujuan untuk mengidentifikasi dan mengungkapkan sasaran organisasi, lingkungan dimana sasaran hendak dicapai, stakeholders yang berkepentingan, dan keberagaman kriteria risiko, dimana hal-hal ini akan membantu mengungkapkan dan menilai sifat dan kompleksitas dari risiko. Terdapat empat aktivitas yang perlu dilakukan pada penetapan konteks, yaitu penetapan konteks internal, konteks eksternal, konteks proses manajemen risiko, dan membangun kriteria risiko.

2) Penilaian risiko (*risk assessment*)

Penilaian risiko terdiri dari:

i) Identifikasi risiko

Di dalamnya memuat proses identifikasi risiko yang dapat mempengaruhi pencapaian sasaran organisasi atau jika di dalam proyek

keberadaannya dapat mengganggu keberlangsungan proyek. Dicari tahu asal / sumber risiko, waktu terjadinya, dan area mana saja yang terdampak, apa penyebab dan potensi risikonya sejauh apa.

ii) Analisis risiko

Di dalamnya memuat proses analisis kemungkinan dan dampak dari risiko yang telah diidentifikasi, menentukan besar konsekuensi yang akan diterima, kemungkinan munculnya risiko, dan menghitung tingkat / level risiko. Pemberian skor (nilai) adalah dengan membandingkan frekuensi kejadian dan dampak yang diakibatkan ditunjukkan pada Tabel 2.3 di bawah ini:

Tabel 2.3 *Risk Matrix*

Dampak / Frekuensi	1 Sangat kecil	2 Kecil	3 Biasa	4 Besar	5 Sangat besar
5 Sering terjadi	Sedang	Sedang	Tinggi	Ekstrim	Ekstrim
4 Sering	Rendah	Sedang	Tinggi	Tinggi	Ekstrim
3 Biasa	Rendah	Sedang	Sedang	Tinggi	Tinggi
2 Jarang	Rendah	Rendah	Sedang	Sedang	Tinggi
1 Sangat jarang	Rendah	Rendah	Rendah	Rendah	Sedang

Penilaian yang dilakukan kemungkinan besar bersifat subyektif, untuk itu dibantu dengan mengumpulkan data dan informasi berupa pengalaman yang dimiliki tim, peristiwa/kejadian yang sudah terjadi sebelumnya, survei, dan lain-lain.

iii)Evaluasi risiko

Di dalamnya memuat aktivitas yang membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan bagaimana penanganan risiko yang akan diterapkan serta membuat tabel prioritas penanganan risiko.

3) Penanganan risiko (*risk treatment*)

Tahap ini menyeleksi metode penanganan dari empat metode yang bisa dipilih yaitu, menghindari risiko (*risk avoidance*), mitigasi risiko (*risk reduction*), transfer risiko kepada pihak ketiga (*risk sharing*), atau menerima risiko (*risk acceptance*).

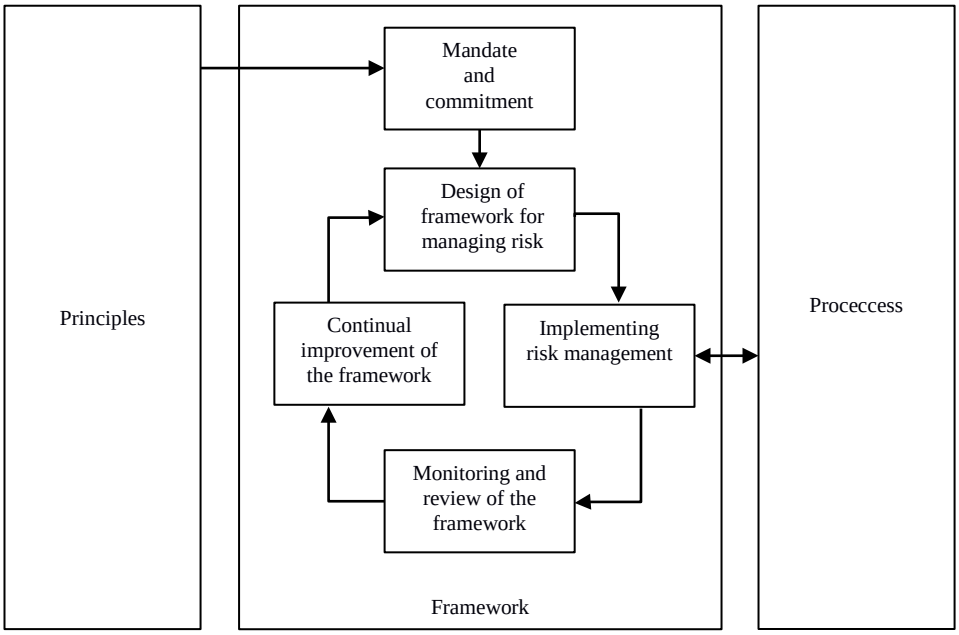
4) Komunikasi dan konsultasi

Komunikasi dan konsultasi merupakan hal yang penting mengingat prinsip manajemen risiko yang kesembilan menuntut manajemen risiko yang transparan dan inklusif, dimana manajemen risiko harus dilakukan oleh seluruh bagian organisasi dan memperhitungkan kepentingan dari seluruh stakeholders organisasi. Adanya komunikasi dan konsultasi diharapkan dapat menciptakan dukungan yang memadai pada kegiatan manajemen risiko dan membuat kegiatan manajemen risiko menjadi tepat sasaran.

5) *Monitoring* dan *review*

Hal ini diperlukan untuk memastikan bahwa implementasi manajemen risiko telah berjalan sesuai dengan perencanaan yang dilakukan. Hasil monitoring dan review juga dapat digunakan sebagai bahan pertimbangan untuk melakukan perbaikan terhadap proses manajemen risiko.

Mandate/commitment memuat prinsip yang isinya telah dijelaskan pada paragraf di awal sub bab ini memiliki keterkaitan langsung dengan prinsip-prinsip ISO 31000. Sedangkan Implementasi dari manajemen risikonya berkaitan langsung terhadap proses manajemen risiko. Relasi (keterhubungan) antara prinsip, kerangka kerja (*framework*), dan proses manajemen risiko pada ISO 31000 ditunjukkan pada Gambar 2.1 4 berikut ini.



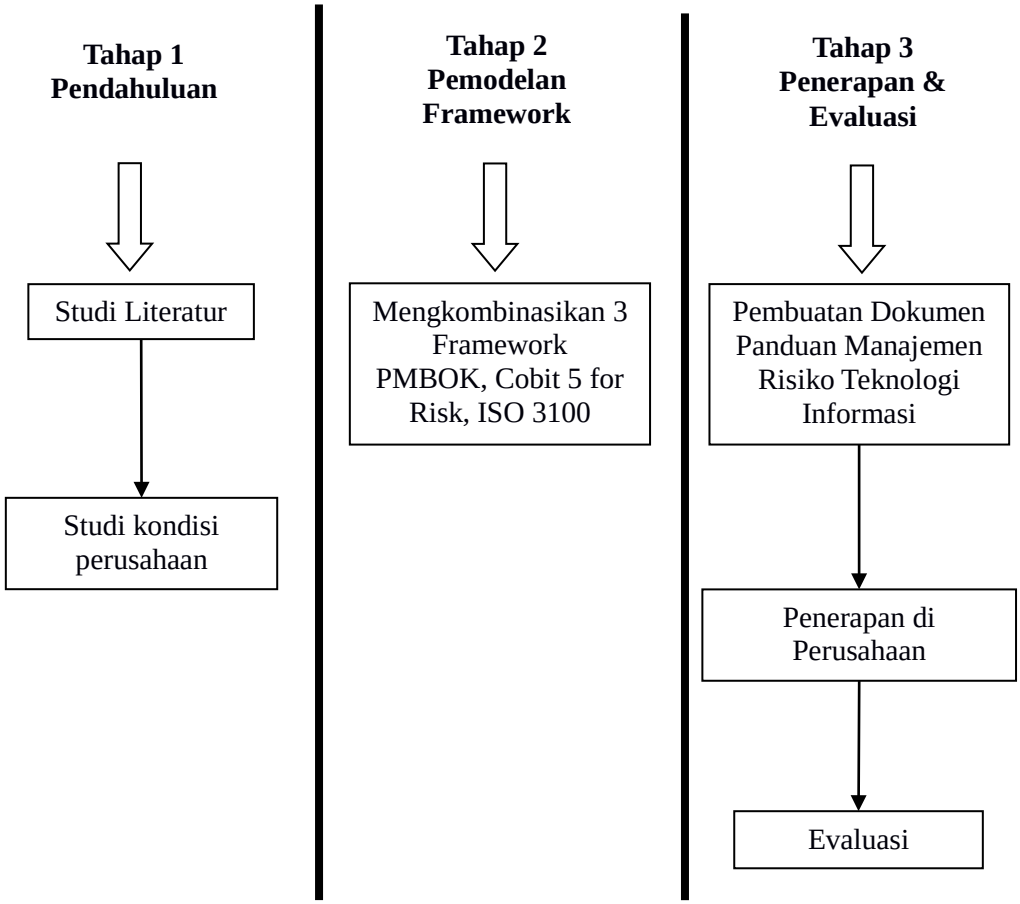
Gambar 2.14 Relasi (keterhubungan) antara prinsip, kerangka kerja (framework), dan proses manajemen risiko pada ISO 31000

Keberadaan prinsip manajemen risiko diatas, disertai penetapan konteks eksternal dan pemisahan antara kerangka kerja dengan proses manajemen risiko menjadi keunggulan kompetitif yang dimiliki oleh ISO 31000: 2009. Diharapkan hal tersebut dapat meningkatkan memaksimalkan proses penyusunan manajemen risiko pada penelitian ini.

Halaman ini sengaja dikosongkan

BAB 3
METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan dalam penelitian ini tampak pada Gambar 3.1 di bawah ini.



Gambar 3.1 Tahap Metodologi Penelitian

3.1 Tahap pendahuluan

Tahap ini terdiri dari studi literatur dan studi kondisi perusahaan.

3.2.1 Studi literatur

Proses ini dilakukan untuk mempelajari hal-hal yang berkaitan dengan manajemen risiko teknologi informasi. Studi literatur yang dilakukan

menggunakan sumber dari buku dan jurnal yang membahas tentang manajemen risiko teknologi informasi, PMBOK, COBIT 5 *for Risk*, dan ISO 31000. Pembahasan mengenai studi literatur ada di Bab 2 Teori dan Kajian Pustaka yang membahas mengenai Manajemen risiko, PMBOK, COBIT 5 *for Risk*, dan ISO 31000.

3.2.2 Studi kondisi perusahaan

Proses ini merupakan kegiatan pengumpulan data di lapangan melalui pembuatan daftar permasalahan teknologi informasi yang memiliki keterkaitan dengan proyek perusahaan XYZ melalui wawancara dengan manajer TI mengenai risiko-risiko yang sering terjadi selama fase awal proyek. Dari proses wawancara dapat diketahui bahwa risiko yang sering terjadi pada fase awal banyak yang terkait dengan TI dan hal ini rentan menimbulkan dampak terhadap kelangsungan dan kelancaran proyek. Diantaranya adalah penginputan data ukuran bangunan harus benar, perhitungan harus tepat, desain harus selesai tepat waktu, pembuatan spesifikasi teknis dan metode pelaksanaan pekerjaan harus cepat, perhitungan kebutuhan material Aluminium Composite Panel harus sesuai dengan volume yang diperlukan, serta pengiriman dokumen teknis (rencana gambar, kontrak kerja, dan sebagainya) melalui email harus dipastikan benar-benar terkirim pada klien. Dari studi mengenai kondisi perusahaan diatas dapat diketahui bahwa setiap kegiatan masing-masing diatas memiliki risiko gagal sehingga dibutuhkan antisipasi untuk mencegah dan mengurangi risiko-risiko tersebut agar proyek terus berjalan dengan lancar.

3.2 Tahap pemodelan framework

Pada tahap ini dilakukan pemodelan *framework* menggunakan acuan PMBOK, COBIT 5 *for Risk*, dan ISO 31000. Dari penelitian yang sudah ada, upaya mengintegrasikan beberapa *framework* dipandang bisa memberikan hasil yang paling efisien dan aplikatif bagi perusahaan yang mencoba untuk mengadopsi *framework-framework* tersebut.

Buku terbitan *IT Governance Institute* yang berjudul *Mapping of PMBOK with COBIT* menjabarkan bagaimana memetakan proses pada PMBOK

ke dalam proses yang terdapat pada COBIT. Dimana masing-masing proses dinilai melalui seberapa banyak proses yang terlibat, lalu hasilnya dituangkan ke dalam tabel. Dari tabel tersebut dapat diketahui bahwa PMBOK unggul dalam proses inisiasi fase proyek, dimana COBIT tidak memiliki penjelasan yang rinci mengenai hal tersebut. Tetapi COBIT unggul dalam merinci proses inisiasi aktivitas-aktivitas yang terkait dengan TI. Sedangkan ISO 31000 pada penelitian ini akan dimanfaatkan prinsip-prinsipnya pada saat menyusun panduan manajemen risiko tersebut. Tujuan pemetaan tersebut adalah untuk mendorong proses dan mengembangkannya.

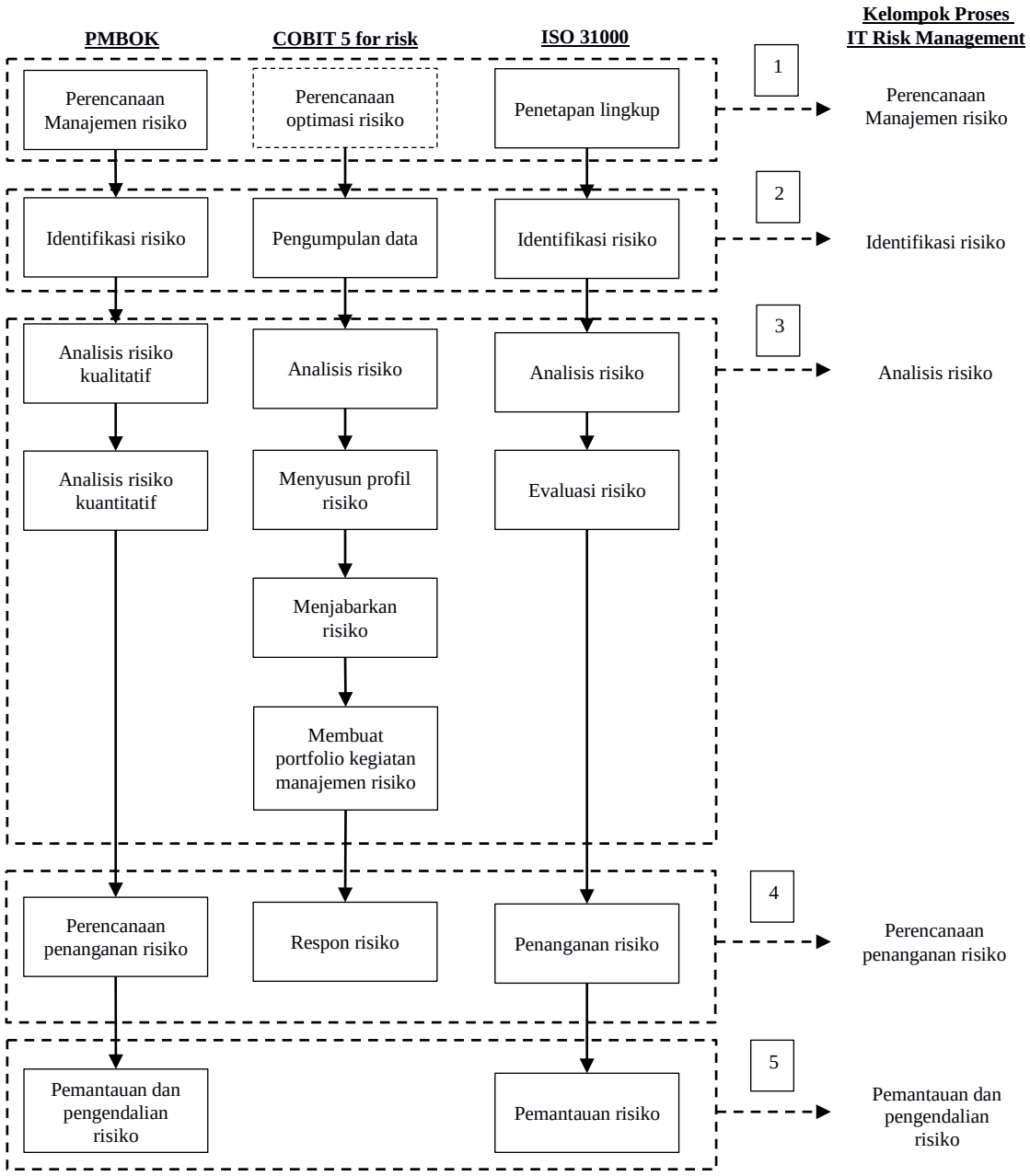
Sedangkan pada jurnal penelitian "*Towards a New Approach For Combining the IT Framework*" metode kombinasi yang dilakukan adalah dengan membandingkan proses, *best practices*, dan pemetaan untuk standar TI. Di dalamnya ditemukan beberapa persamaan pada beberapa *framework* yang dipakai. Setiap *framework*, baik sebagian kecil ataupun keseluruhan digunakan untuk meningkatkan pelayanan TI dan produktivitas bisnis.

Dalam buku COBIT *5 for Risk* disebutkan bahwa COBIT mampu mengcover proses manajemen risiko pada ISO 31000. Dari kedua buku tersebut dapat disimpulkan bahwa COBIT mampu mengcover PMBOK dan ISO 31000 dalam hal manajemen risiko. Jadi apa kekurangan yang dimiliki COBIT dibanding keduanya? Dan apa kelebihan PMBOK serta ISO 31000 dibanding COBIT? Seperti telah kita ketahui diawal bahwasanya COBIT tidak memberikan panduan implementasi operasional pada manajemen risikonya. COBIT hanya memberikan panduan "apa saja yang harus dikontrol" ketimbang "*how-to-control*" atau cara melakukannya. Sedangkan PMBOK dan ISO 31000 dengan jelas memberikan "*how-to*"-nya. Sebagai contoh, dalam tahap analisis risiko PMBOK menjelaskan opsi yang bisa dipakai antara lain menggunakan matriks risiko, sedangkan dalam COBIT hanya dijelaskan aktivitasnya adalah analisis tanpa menjelaskan model metodenya.

PMBOK, COBIT, dan ISO 31000 sama-sama memiliki tahap/proses untuk mengelola risiko. Sebelum disusun tahapan proses manajemen risiko TI melalui kombinasi ketiganya, terlebih dahulu masing-masing proses pengelolaan risiko dari ketiganya dipilih untuk menjadi proses terpilih. PMBOK akan dipakai

sebagai *guidance* utama dalam pemilihan proses ini. Urutannya adalah, PMBOK akan dibandingkan dengan COBIT, kemudian setelah itu akan dibandingkan dengan ISO 31000. Proses-proses yang memiliki kesamaan aktivitas atau dinilai aktivitasnya mirip, akan digabung ke dalam kelompok yang sama.

Pengkombinasiannya dilakukan melalui pengelompokan proses dari *PMBOK, COBIT 5* for Risk, *dan ISO 31000* seperti pada Gambar 3.2 di bawah ini.



Gambar 3.2 Pengelompokan proses manajemen risiko teknologi informasi dengan PMBOK, COBIT 5 *for Risk*, dan ISO 31000

Masing-masing *framework* akan berperan sesuai dengan keunggulannya masing-masing. Dari awal telah dijelaskan bahwa keunggulan yang dimiliki PMBOK dalam penelitian ini adalah memiliki penjelasan cara (*how-to*) dalam mengelola risiko. PMBOK akan digunakan untuk menyusun fase proses manajemen risiko yang disesuaikan dengan proyek perusahaan XYZ karena PMBOK mampu mencakup setiap fase dalam proyek yang dijalankan perusahaan XYZ. Namun untuk rincian aktivitas TI di setiap fase, COBIT memiliki gambaran yang lebih lengkap, seperti operasional TI, keamanan TI, dan sebagainya sehingga cocok untuk mendetilkan bagian teknologi informasi dalam setiap fase yang dihasilkan oleh PMBOK. Jika COBIT 5 *for risk* merupakan bagian dari COBIT dan manajemen risiko proyek merupakan bagian dari PMBOK, maka berbeda dengan ISO 31000 yang berdiri sendiri dan memang khusus dibuat untuk panduan manajemen risiko. Oleh karena itu pada ISO 31000 terdapat pemisahan yang jelas antara prinsip, *framework,* dan proses dalam manajemen risiko. Inilah salah satu kelebihan ISO 31000 dibanding yang lain.

Adapun penjelasan mengenai kombinasi pada setiap kelompok proses *IT risk management* adalah sebagai berikut:

1. Perencanaan Manajemen Risiko

   Pada tahap ini PMBOK, COBIT 5 *for Risk,* dan ISO 31000 akan dikombinasikan dengan cara membandingkan proses masing-masing. PMBOK memiliki proses perencanaan manajemen risiko dan ISO 31000 memiliki proses penetapan lingkup yang mirip dengan proses perencanaan risiko. Sedangkan pada COBIT 5 *for Risk* memiliki perencanaan optimasi risiko, tetapi tidak dimasukkan ke dalam proses melainkan *risk governance*. Hal ini karena pada COBIT antara *governance* dan manajemen diletakkan secara terpisah. Oleh karena itu yang digunakan pada tahap ini adalah PMBOK dan ISO 31000.

2. Identifikasi Risiko

   Pada tahap ini PMBOK memiliki proses identifikasi risiko yang meliputi input, tool, dan output. COBIT memiliki proses pengumpulan data yang meliputi pembuatan *risk scenario,* yaitu daftar kemungkinan kejadian risiko positif dan negatif yang dikelompokkan berdasar jenis (kategori) risiko.

COBIT telah memiliki pembagian jenis risiko menjadi 20 macam. Sedangkan ISO 31000 memiliki proses identifikasi risiko yang menyediakan pertanyaan 5W (*What, Who, Where, When*, dan *Why*) + 1H (*How*) untuk mendaftar risiko yang sedang terjadi dan yang mungkin terjadi. Dari ketiganya proses pengumpulan data COBIT dinilai lebih lengkap karena risikonya telah terkategorisasi secara IT. Sehingga pada tahap ini proses yang dipakai adalah proses dari COBIT.

3. Analisis Risiko

   Pada tahap ini PMBOK memiliki proses analisis kualitatif dan analisis kuantitatif yang disertai beberapa jenis metode yang bisa dipakai. COBIT 5 *for Risk* memiliki proses analisis tetapi di dalamnya tidak menjelaskan detil metode yang harus digunakan untuk menganalisa. ISO 31000 memiliki proses analisis dan memberikan penjelasan cara melakukan analisa risiko dengan rinci. Oleh karena itu pada tahap ini dipilih PMBOK dan ISO 31000 karena menyediakan beberapa pilihan metode analisis risiko beserta detilnya.

4. Perencanaan Penanganan Risiko

   Pada tahap ini PMBOK, COBIT 5 *for Risk*, dan ISO 31000 memiliki opsi respon yang sama terhadap risiko yaitu terhadap risiko negatif terdapat opsi *avoid, reduce, transfer/sharing,* dan *accept*. Sedangkan untuk risiko positif terdapat opsi *exploit, enhance, share*, dan *ignore*. Sehingga pada tahap ini dari ketiganya bisa dipilih salah satu.

5. Pemantauan dan Pengendalian Risiko

   Pada tahap ini PMBOK, COBIT 5 *for Risk*, dan ISO 31000 sama-sama memiliki proses pemantauan dan pengendalian risiko. Hanya saja dalam PMBOK dan COBIT 5 *for Risk* aktivitas pemantauan dan pengendalian risiko diletakkan di akhir proses, sedangkan pada ISO 31000 aktivitas pemantauan dan pengendalian risiko wajib ada di setiap tahap proses. Sehingga dipilihlah proses ISO 31000 pada tahap ini karena aktivitas setiap tahap proses bisa dipantau dan dikendalikan.

Proses-proses yang terpilih dapat disimpulkan seperti yang disajikan pada Tabel 3.1. Kemudian kelima proses yang telah dikombinasikan akan disusun menjadi alur proses manajemen risiko.

Tabel 3.1 Penilaian proses yang mendukung manajemen risiko TI pada perusahaan XYZ

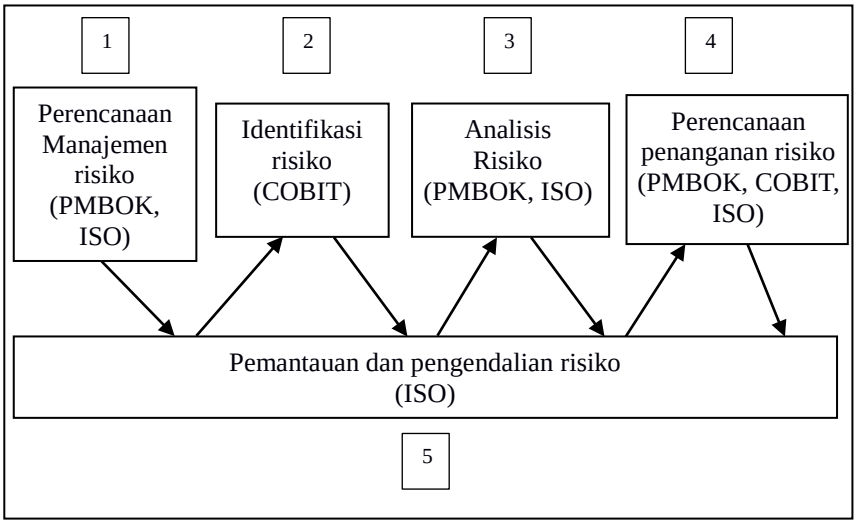
	PMBOK	COBIT	ISO 31000
Perencanaan Manajemen Risiko	●	○	●
Identifikasi Risiko	◖	●	◖
Analisis Risiko	●	◖	●
Perencanaan penanganan Risiko	●	●	●
Pemantauan dan pengendalian Risiko	◖	◖	●

Ket. : ○: kurang mendukung

◖ : cukup mendukung

●: sangat mendukung

Dari pembahasan Tabel 3.1 di atas diperoleh hasil kombinasi dari manajemen risiko PMBOK, COBIT 5 *for Risk*, dan ISO 31000 seperti ditunjukkan pada Gambar 3.3 berikut ini:



Gambar 3.3 Hasil kombinasi manajemen risiko teknologi informasi dengan PMBOK, COBIT 5 *for Risk*, dan ISO 31000

Penjelasan mengenai Gambar 3.3 diatas akan dijabarkan sebagai berikut:

3.2.1 Perencanaan manajemen risiko

Tahapan perencanaan manajemen risiko ini menggabungkan tahap perencanaan manajemen risiko milik PMBOK dan penetapan lingkup (*establishing context*) ISO 31000. Perencanaan manajemen risiko PMBOK mengaitkan risiko pada IT dengan daur hidup proyek, mulai dari penyesuaian dengan jadwal proyek, jumlah sumber daya, dan sebagainya. Untuk penetapan lingkup ISO 31000 dimulai dengan mempelajari kondisi perusahaan baik internal maupun eksternal dan membangun kriteria risiko. Dari tahap ini dilanjutkan ke tahap pemantauan dan pengendalian untuk memantau apakah ada koreksi baik dari tingkat direksi, manajemen, atau unit kerja perusahaan.

3.2.2 Pemantauan dan pengendalian risiko

Setelah tahap perencanaan manajemen risiko dibuat selanjutnya dilakukan pemantauan dan pengendalian dengan mengirimkan laporan dokumentasi hasil dari tahap perencanaan kepada direksi dan manajemen untuk mendapatkan persetujuan. Jika tidak ada revisi maka bisa dilanjutkan pada tahap berikutnya yaitu identifikasi risiko.

3.2.3 Identifikasi risiko

Pada tahap ini digunakan *risk scenario* milik COBIT 5 *for Risk* karena di dalamnya mampu merinci kejadian risiko lebih detil. *Risk scenario* berisi kemungkinan kejadian risiko yang mungkin terjadi yang dikelompokkan berdasar jenis (kategori) risiko TI. Pada PMBOK dan ISO 31000 tahap identifikasinya tidak sedetil COBIT. Kemudian dilanjutkan ke tahap monitor kontrol reviu untuk mengecek ulang apakah *risk scenario* sudah komplit atau belum.

3.2.4 Pemantauan dan pengendalian risiko

Setelah tahap identifikasi risiko dibuat selanjutnya dilakukan pemantauan dan pengendalian dengan mengirimkan laporan dokumentasi hasil dari tahap identifikasi risiko kepada direksi dan manajemen untuk mendapatkan persetujuan.

Jika tidak ada revisi maka bisa dilanjutkan pada tahap berikutnya yaitu analisis risiko.

3.2.5 Analisis risiko

Tahap ketiga adalah analisis risiko yaitu penilaian risiko yang sudah didaftarkan sebelumnya agar diketahui seberapa tinggi efek/dampaknya. Pada tahap ini PMBOK membagi analisis risiko menjadi dua yaitu, analisis risiko kualitatif dan analisis risiko kuantitatif. Analisis kualitatif dibuat untuk memberikan gambaran umum tentang level risiko. Analisis kualitatif menggunakan bentuk kata atau skala deskriptif untuk menjelaskan seberapa besar potensi risiko yang diukur. Apakah termasuk level risiko rendah, sedang, atau tinggi. Pada analisis kuantitatif yang digunakan adalah nilai numerik. Probabilitas/frekuensi kejadian beserta dampaknya dituangkan dalam bentuk numerik untuk menentukan tingkatan risikonya. Pada ISO 31000 ada satu lagi tambahan yaitu analisis semi kuantitatif, yaitu dari penilaian skala kualitatif yang telah disebutkan diatas diberi nilai yang menggambarkan besaran kemungkinan maupun dampak risiko. Hasilnya berupa tingkat risiko yang merupakan perkalian dari keduanya. Pada ISO 31000 proses analisis ini diikuti oleh tahap evaluasi risiko yang bertujuan untuk mendapatkan data *risk residual* setelah dilakukan penanganan risiko.

3.2.6 Pemantauan dan pengendalian risiko

Setelah tahap analisis risiko dibuat selanjutnya dilakukan pemantauan dan pengendalian dengan mengirimkan laporan dokumentasi hasil dari tahap analisis risiko kepada direksi dan manajemen untuk mendapatkan persetujuan. Jika tidak ada revisi maka bisa dilanjutkan pada tahap berikutnya yaitu perencanaan penanganan risiko.

3.2.7 Perencanaan penanganan risiko

Tahap ini merupakan tahap untuk memilih opsi penanganan terhadap risiko. Opsi yang bisa dipilih yaitu *accept, mitigate, transfer,* dan *avoid* untuk risiko negatif, dan untuk risiko positif terdapat opsi *exploit, enhance, share,* dan *ignore*.

3.2.8 Pemantauan dan pengendalian risiko

Setelah tahap perencanaan manajemen risiko dibuat selanjutnya dilakukan pemantauan dan pengendalian dengan mengirimkan laporan dokumentasi hasil dari tahap perencanaan penanganan risiko kepada direksi dan manajemen untuk mendapatkan persetujuan. Sebagai tambahan, pada tahap ini risiko-risiko yang ada terus diawasi *residual risk* atau risiko yang masih tersisa dan dilakukan pengendalian untuk meminimalisir dampak dan kemungkinan kejadiannya. Hal inilah yang membedakan tahap pemantauan ini dengan tahap pemantauan yang sebelum-sebelumnya.

3.3 Tahap Penerapan & Evaluasi

Tahap ini merupakan penerapan / implementasi panduan manajemen risiko TI yang telah dibuat. Pada proses implementasi, data yang digunakan akan diambil dari survei kejadian yang sedang berlangsung di proyek dan juga catatan sejarah (*history*) pada proyek-proyek sebelumnya.

Kendala-kendala yang berada di wilayah teknologi informasi baik yang sudah terjadi atau sedang terjadi dideskripsikan dan ditulis. Kemungkinan kendala yang terjadi di masa depan juga dicatat untuk mencegah atau mengurangi dampak buruknya terhadap kelangsungan proyek perusahaan. Risiko-risiko yang mungkin belum tercatat bisa digali lebih banyak melalui wawancara dengan manajer tim TI. Wawancara ini berguna untuk melengkapi risik-risiko krusial yang berkaitan dengan TI pada proyek perusahaan XYZ. Wawancara ini juga berguna untuk menilai apakah suatu risiko memiliki tingkat risiko tinggi, sedang, atau rendah.

Pada saat penerapan atau implementasi ini akan dilakukan evaluasi yang berupa penilaian apakah panduan manajemen risiko teknologi informasi yang telah dibuat mudah dimengerti dan mudah diterapkan oleh tim divisi TI perusahaan XYZ. Penilaiannya dilakukan melalui pembagian kuesioner kepada *end user* (staf IT) yang berisi pertanyaan mengenai kemudahan penerapan/penggunaan pedoman manajemen risiko teknologi informasi yang telah dibuat tersebut.

BAB 4
ANALISA DAN PEMBAHASAN

Pada bab ini akan dianalisis hasil dari penerapan panduan manajemen risiko TI pada proyek perusahaan XYZ dan hasil kuesioner kemudahan penggunaan panduan. Urutan tahap panduan adalah perencanaan manajemen risiko, identifikasi risiko, analisis risiko, perencanaan penanganan risiko, serta pemantauan dan pengendalian risiko.

4.1 Perencanaan Manajemen Risiko

Pada tahap ini dasar yang dipakai adalah dari PMBOK dan ISO 31000. Berdasar PMBOK tahap perencanaan manajemen risiko berisi rencana dasar untuk menghadapi risiko. Yang dijadikan input atau landasan/pijakan pada tahap ini adalah rencana manajemen proyek, kontrak/perjanjian pekerjaan, kondisi lingkungan perusahaan, dan proses organisasi. Dimana outputnya adalah berupa rencana manajemen risiko. Hal ini bisa dilakukan melalui rapat perencanaan dan analisis. Template berupa penetapan *risk appetite* dan *risk tolerance*, tabel untuk mendefinisikan level risiko, kemungkinan (*probability*), dampak (*impact*), dan matrik perkalian kemungkinan dan dampak dibuat untuk diisikan nanti pada tahap analisis risiko.

Maksud dan tujuan dilakukan penentuan *Risk Appetite* dan *Risk Tolerance* adalah untuk memberikan pedoman limit/ambang batas dan toleransi risiko yang diperbolehkan dalam rangka pengendalian risiko untuk menghindari potensi kerugian yang lebih besar. *Risk Appetite* dan toleransi risiko ditentukan terhadap semua kemungkinan kejadian risiko yang diperkirakan dapat menimbulkan kerugian atau kegagalan proyek dan atau hilangnya kesempatan meraih keuntungan perusahaan.

Pernyataan *risk appetite* TI perusahaan XYZ adalah sebagai berikut:

1. Suatu risiko hanya diterima jika potensi keuntungan melebihi biaya yang dikeluarkan.
2. Perusahaan tidak menerima risiko yang berpotensi menimbulkan kerugian

keuangan yang besar atau kerugian reputasi perusahaan.

Risk tolerance atau toleransi risiko biasanya disebut juga limit toleransi, yaitu tingkat variasi relatif kejadian risiko yang dapat diterima untuk pencapaian tujuan strategis perusahaan/organisasi atau tingkat dimana kejadian risiko yang terjadi tidak akan menggangu pencapaian tujuan perusahaan/organisasi. Berdasarkan *Risk Appetite* tersebut, perusahaan XYZ membuat pernyataan *Risk Tolerance* sebagai berikut :

1. Toleransi derajat kesalahan perhitungan kebutuhan material hanya diperkenankan maksimum 5%.
2. Kesalahan apapun yang menyebabkan proyek terganggu dengan sengaja tidak dapat diterima/ditoleransi.

Setelah menetapkan *risk appetite* dan *risk tolerance*, selanjutnya bisa dibuat template tabel kemungkinan, dampak, dan perkalian dampak dan risiko. Tabel 4.1 berikut ini mendefinisikan level kemungkinan muncul atau terjadinya risiko yang dibuat oleh tim IT perusahaan XYZ.

Tabel 4.1 Level Kemungkinan

Level	Kemungkinan	Uraian
1	Jarang	Probabilitas kejadian ≤ 20%
2	Kemungkinan kecil	Probabilitas kejadian 20% < x ≤ 40%
3	Kemungkinan sedang	Probabilitas kejadian 40% < x ≤ 60%
4	Kemungkinan besar	Probabilitas kejadian 60% < x ≤ 80%
5	Hampir pasti	Probabilitas kejadian 80% < x ≤ 100%

Tabel 4.1 di atas berfungsi untuk menentukan standar ukuran dari probabilitas kejadian dari risiko TI. Besar probabilitas kejadian bersifat fleksibel disesuaikan dengan preferensi perusahaan. Untuk tingkatan levelnya secara umum terdiri dari lima level seperti disebutkan pada tabel tersebut.

Tabel lain yang dibuat adalah level dampak yang mendefinisikan level dampak ketika risiko terjadi. Berikut ini adalah Tabel 4.2 memperlihatkan level dampak atau pengaruh terhadap proyek ketika ada risiko yang terjadi pada TI yang dibuat oleh tim IT perusahaan XYZ.

Tabel 4.2 Level Dampak

Level	Dampak	Uraian
1	Tidak signifikan	Dampaknya dapat ditangani dan tidak mempengaruhi kelancaran proyek
2	Kecil	Sedikit mempengaruhi kelancaran proyek
3	Sedang	Mengganggu kelancaran proyek
4	Besar	Kerugian cukup besar terhadap keberlangsungan proyek dan perusahaan
5	Luar biasa	Menimbulkan bencana/kerugian yang sangat besar pada proyek

Tabel 4.2 di atas fungsinya mirip pada tabel level kemungkinan yaitu untuk menentukan standar ukuran dari probabilitas dampak kejadian risiko TI. Masing-masing uraian diatas bersifat fleksibel disesuaikan dengan preferensi perusahaan. Untuk tingkatan levelnya secara umum terdiri dari lima level seperti disebutkan pada tabel tersebut.

Selanjutnya, berdasar ISO 31000 tahap perencanaan manajemen risiko disejajarkan dengan penetapan ruang lingkup. Dimana pada ISO 31000 tahap ini terdiri dari empat aktivitas yaitu, penetapan ruang lingkup internal, penetapan ruang lingkup eksternal, penetapan ruang lingkup proses manajemen risiko, dan membangun kriteria risiko sebagai batasan dalam melakukan pengelolaan risiko.

Berikut ini Tabel 4.3 Ruang lingkup yang menjelaskan ruang lingkup internal, ruang lingkup eksternal, dan ruang lingkup proses manajemen risiko.

Tabel 4.3 Ruang lingkup

Ruang Lingkup Internal	Meliputi aktivitas TI yang ada di unit kerja TI yang berhubungan dengan proyek
Ruang Lingkup Eksternal	Meliputi perubahan agreement dengan pemilik proyek yang mempengaruhi aktivitas TI dan berpotensi menimbulkan risiko TI
Ruang Lingkup Manajemen Risiko	Meliputi risiko yang berkaitan dengan aktivitas TI dan mempengaruhi kelancaran dan keberhasilan proyek

Selanjutnya di bawah ini adalah Tabel 4.4 Kriteria Risiko yang mendefinisikan tingkat risiko dari yang rendah hingga ekstrim beserta penjelasannya.

Tabel 4.4 Kriteria Risiko

Level Risiko	Kriteria	Uraian
Rendah	Dapat diterima dan dilakukan pemantauan	Dibutuhkan pengendalian normal
Sedang	Perlu pengendalian risiko	Dibutuhkan pengendalian yang baik
Tinggi	Perlu pengendalian yang ketat	Dibutuhkan pengendalian yang sangat baik (*excellent*)
Ekstrim	Tidak dapat diterima	Dibutuhkan pengendalian yang sangat baik (*excellent*)

4.2 Identifikasi Risiko.

Identifikasi risiko dalam penelitian ini merupakan proses untuk menjaring setiap risiko yang berpotensi menghambat pencapaian tujuan dan sasaran TI pada perusahaan sehingga tidak ada risiko potensial yang tidak teridentifikasi. Pada tahap ini akan dilakukan identifikasi risiko untuk mengenali dan menemukan jawaban terhadap apa, bagaimana, kapan, dan mengapa mengenai risiko TI dan juga mengenai penyebab risiko itu terjadi serta dampak resiko yang ditimbulkannya.

Mengacu kepada standar COBIT 5 *for Risks*, terdapat dua puluh jenis (kategori) risiko TI untuk setiap risiko yang diidentifikasi, berikut merupakan pembagian dua puluh jenis risiko tersebut yang disajikan pada Tabel 4.5 berikut:

Tabel 4.5 Pembagian Jenis (Kategori) Risiko

No	Kategori	Pengertian
1	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio
2	*Programme/ projects life cycle management (programme/ project initiation, economics, delivery, quality and termination)*	Manajemen siklus hidup program atau proyek (inisiasi program/proyek, biaya, delivery, kualitas dan penutupan proyek)
3	*IT investment decision making*	Pengambilan keputusan investasi TI
4	*IT expertise and skills*	Ketrampilan dan keahlian TI
5	*Staff operations (human error and malicious intent)*	Staff operasional (kesalahan faktor manusia disengaja maupun tidak)

6	*Information (data breach: damage, leakage and access)*	Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)
7	*Architectural (vision and design)*	Arsitektur (visi dan desain)
8	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*	Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)
9	*Software*	Perangkat lunak
10	*Business ownership of IT*	Kepemilikan bisnis TI
11	*Supplier selection/performanse, contractual compliance, termination of service and transfer*	Pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan
12	*Regulatory compliance*	Pemenuhan regulasi
13	*Geopolitical*	Geopolitik
14	*Insfrastructure theft or destruction*	Pencurian infrastruktur atau pengrusakan
15	*Malware*	Malware
16	*Logical attacks*	Serangan langsung pada sistem, perangkat lunak, ataupun data
17	*Industrial action*	Situasi dalam dunia industri
18	*Environmental*	Lingkungan
19	*Acts of Nature*	Bencana alam
20	*Innovation*	Inovasi

Identifikasi risiko ini mengacu pada COBIT tahap pengumpulan data. Yang perlu dilakukan pada tahap ini adalah membuat *risk scenario*. Berikut ini adalah hasil dari pengidentifikasian risiko pada proyek dari tahun 2014 hingga sekarang melalui pembuatan Tabel 4.6 *Risk Scenario*:

Tabel 4.6 *Risk scenario*

No	Jenis Risiko	Tipe Risiko			Skenario Risiko	
		IT benefit / value enablement risk	*IT programme and project delivery risk*	*IT operations and service delivery risk*	Skenario Negatif	Skenario Positif
1	*IT Expertise and skill*	P	S	P	Staf merangkap tugas	Staf memiliki tugas yang jelas dan tidak merangkap
2		P	S	P	Jumlah SDM terbatas	Jumlah SDM sesuai dengan banyaknya beban kerja.
3		S	P	P	Skill staf masih kurang	Staf memiliki skill yang cukup baik
4		S	P	P	Tidak ada pelatihan / training untuk meningkatkan skill staf	Ada pelatihan reguler untuk meningkatkan skill staf
5		S	P	P	Tidak ada transfer knowledge dari staf yang resign ke staf baru	Ada proses transfer knowledge dari staf yang resign ke staf baru
6	*Staff operation (human error and malicious intent)*	S	S	P	Staf lalai dan menyebabkan kerusakan pada hardware	Ada pelindung di semua hardware
7		S	S	P	Staf salah dalam membaca ukuran gambar	Ada pemeriksa
8		S	S	P	Kesalahan dalam menghitung kebutuhan material (BoQ)	Ada pemeriksa

No	Jenis Risiko	Tipe Risiko			Skenario Risiko	
		IT benefit / value enablement risk	*IT programme and project delivery risk*	*IT operations and service delivery risk*	Skenario Negatif	Skenario Positif
9		S	S	P	Keterlambatan staf dalam sharing info kebutuhan material	Cepat dalam sharing info kebutuhan material
10	*Information*	P	S	P	Data hilang (tidak ada backup)	Backup data rutin
11		S	S	P	Data dari owner tidak lengkap	Ada proses ceklist data gambar yang masuk
12		S	S	P	Adanya informasi yang hilang saat ada staf resign mendadak	Ada sharing informasi dan laporan pekerjaan
13	*Infrastructure*	P	S	S	Spesifikasi hardware rendah	Spesifikasi hardware sesuai kebutuhan
14		S	S	P	Penyimpanan data tidak teratur menyebabkan pencarian sulit	Membuat database
15	*Software*	S	P	S	Software tidak update	Software selalu update
16		P	P	S	Software rusak	Ada backup software
17	*Malware*	S	S	P	Ada serangan malware	Ada perlindungan terhadap malware
18	*Logical attack*	S	S	P	Ada serangan virus	Ada anti virus yang terus update
19	*IT investment and decision making*	S	S	P	Belum ada portal internal untuk sharing info dan	Ada portal khusus untuk sharing info proyek

No	Jenis Risiko	Tipe Risiko			Skenario Risiko	
		IT benefit / value enablement risk	*IT programme and project delivery risk*	*IT operations and service delivery risk*	Skenario Negatif	Skenario Positif
					data proyek real time	
20		S	S	P	Belum semua staf memiliki email internal dan masih menggunakan email pribadi menyebabkan lalu lintas data sulit dipantau	Semua staf memiliki email internal
21		S	S	P	Belum ada aplikasi sebagai alat bantu untuk menghitung kebutuhan material	Ada alat bantu hitung kebutuhan material
22	*Regulatory compliance*	P	S	S	Belum ada regulasi tertulis untuk penanganan masalah IT	Ada aturan tertulis untuk penanganan masalah IT
23	*Architecture*	P	S	S	Belum ada perangkat keamanan TI	Ada perangkat keamanan TI
24		S	S	P	Belum semua PC terhubung dan tersambung ke printer	Semua perangkat sudah terhubung dalam satu jaringan

Pada tabel diatas, *IT benefit / value enablement risk*, diisi dengan ‘P’ (Primer) apabila risiko terkait TI sebagai enabler untuk meningkatkan solusi binis,

sedangkan jika tidak terkait maka diisi dengan ‘S’. *IT programme and project delivery risk*, diisi dengan ‘P’ (Primer) apabila risiko terkait dengan program dan proyek TI, sedangkan jika tidak terkait maka diisi dengan ‘S’. *IT operations and service delivery risk*, diisi dengan ‘P’ (Primer) apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, sedangkan jika tidak terkait maka diisi dengan ‘S’.

4.3 Analisis Risiko

Analisis kualitatif dibuat untuk memberikan gambaran umum tentang level risiko. Analisis kualitatif menggunakan bentuk kata atau skala deskriptif untuk menjelaskan seberapa besar potensi risiko yang diukur. Apakah termasuk level risiko rendah, sedang, atau tinggi. Setelah itu dapat dilakukan analisis semi kuantitatif ataupun kuantitatif untuk lebih merinci level risiko yang ada.

Pada analisis semi kuantitatif, skala kualitatif yang telah disebutkan diatas diberi nilai yang menggambarkan besaran kemungkinan maupun dampak risiko. Hasilnya berupa tingkat risiko yang merupakan perkalian dari keduanya. Sedangkan pada analisis kuantitatif yang digunakan adalah nilai numerik. Probabilitas/frekuensi kejadian beserta dampaknya dituangkan dalam bentuk numerik untuk menentukan tingkatan risikonya. Tabel yang dibuat pada tahap ini adalah Tabel Kriteria Risiko dan Tabel *Risk Map*.

Tabel 4.7 *Risk Map*

Dampak / Kemungkinan	1 Sangat kecil	2 Kecil	3 Biasa	4 Besar	5 Luar biasa
5 Sering terjadi	5 Sedang	10 Sedang	15 Tinggi	20 Ekstrim	25 Ekstrim
4 Sering	4 Rendah	8 Sedang	12 Tinggi	16 Tinggi	20 Ekstrim
3 Biasa	3 Rendah	6 Sedang	9 Sedang	12 Tinggi	15 Tinggi
2 Jarang	2 Rendah	4 Rendah	6 Sedang	8 Sedang	10 Tinggi
1 Sangat jarang	1 Rendah	2 Rendah	3 Rendah	4 Rendah	5 Sedang

Tabel 4.7 *Risk Map* di atas dipakai untuk menentukan tingkat risiko yang diperoleh dari kemungkinan yang dikalikan dengan dampak risiko. Berdasar Tabel 4.7 tersebut diperoleh hasil penentuan kriteria risiko ditunjukkan pada Tabel 4.8 sebagai berikut.

Tabel 4.8 Hasil Kriteria risiko

No (1)	Uraian Risiko (2)	Kemungkinan (3)	Dampak (4)	Kemungkinan x Dampak (5)	Kriteria (6)
1	Staf merangkap tugas	4	2	8	Sedang
2	Jumlah SDM terbatas	3	2	6	Sedang
3	Skill staf masih kurang	3	3	9	Sedang
4	Tidak ada pelatihan / training untuk meningkatkan skill staf	5	2	10	Tinggi
5	Tidak ada transfer knowledge dari staf yang resign ke staf baru	5	3	15	Tinggi
6	Staf lalai dan menyebabkan kerusakan pada hardware	1	3	3	Rendah
7	Staf salah dalam membaca ukuran gambar	2	4	8	Sedang
8	Kesalahan dalam menghitung kebutuhan material (BoQ)	2	4	8	Sedang
9	Keterlambatan staf dalam	4	3	12	Tinggi

No (1)	Uraian Risiko (2)	Kemungkinan (3)	Dampak (4)	Kemungkinan x Dampak (5)	Kriteria (6)
	sharing info kebutuhan material				
10	Data hilang (tidak ada backup)	2	4	8	Sedang
11	Data dari owner tidak lengkap	4	3	12	Tinggi
12	Adanya informasi yang hilang saat ada staf resign mendadak	3	3	9	Sedang
13	Spesifikasi hardware rendah	3	3	9	Sedang
14	Penyimpanan data tidak teratur menyebabkan pencarian sulit	3	3	9	Sedang
15	Software tidak update	1	3	3	Rendah
16	Software rusak	1	3	3	Rendah
17	Ada serangan malware	3	3	9	Sedang
18	Ada serangan virus	3	3	9	Sedang
19	Belum ada portal internal untuk shareing info dan data proyek real time	5	3	15	Tinggi
20	Belum semua staf memiliki email internal	5	3	15	Tinggi

No (1)	Uraian Risiko (2)	Kemungkinan (3)	Dampak (4)	Kemungkinan x Dampak (5)	Kriteria (6)
	dan masih menggunakan email pribadi menyebabkan lalu lintas data sulit dipantau				
21	Belum ada aplikasi sebagai alat bantu untuk menghitung kebutuhan material	3	2	6	Sedang
22	Belum ada regulasi tertulis untuk penanganan masalah IT	4	2	8	Sedang
23	Belum ada perangkat keamanan TI	3	2	6	Sedang
24	Belum semua PC terhubung dan tersambung ke printer	5	2	10	Tinggi

Setelah menentukan kriteria risiko selanjutnya hasil kriteria dimasukkan ke dalam Tabel 4.9 *Risk Map* agar lebih mudah dibaca seperti berikut ini:

Tabel 4.9 Hasil *Risk Map*

Dampak / Kemungkinan	1 Sangat kecil	2 Kecil	3 Biasa	4 Besar	5 Luar biasa
5 Sering terjadi		4,24 ●●	5,19,20 ●●●		
4 Sering		1,22 ●●	9,11 ●●		
3 Biasa		2,21,23 ●●●	3,12,13,14, ●●●●●● 17,18		
2 Jarang				7,8,10 ●●●	
1 Sangat jarang			6,15,16 ●●●		

Dari hasil pemetaan risiko di atas, diperoleh hasil bahwa risiko yang telah diidentifikasi pada tahap awal memiliki tiga macam kriteria risiko yaitu rendah, sedang, dan tinggi. Dimana terdapat tiga macam risiko rendah yang membutuhkan pengendalian normal, enam belas macam dengan risiko sedang yang membutuhkan pengendalian yang baik, dan lima macam dengan risiko tinggi yang membutuhkan pengendalian yang sangat baik. Mengenai respon risiko untuk masing-masing kriteria akan dilakukan pada tahap berikutnya yaitu perencanaan penanganan risiko.

4.4 Perencanaan Penanganan Risiko

Untuk menentukan respon terhadap risiko bisa digunakan metode estimasi/perkiraan secara subyektif. Metode ini disebut *professional judgement* (*Control Self-Assessment Techniques/ CST*). Pemilihan respon terhadap risiko berdasarkan alternatif yang tersedia (*accept, mitigate, transfer, avoid*) untuk risiko negatif, dan untuk risiko positif tersedia *exploit*, *enhance*, *share*, dan *ignore*.

Berikut ini adalah tabel respon risiko yang dibuat oleh tim IT perusahaan XYZ dan berisi perencanaan penanganan untuk tiap-tiap risiko berdasar kriteria risikonya seperti yang ditunjukkan pada Tabel 4.10. Respon yang diberikan ditujukan dengan tujuan manajemen risiko yaitu membantu keberlangsungan dan kelancaran proyek.

Tabel 4.10 Respon risiko

No (1)	Uraian Risiko (2)	Kriteria Risiko (3)	Respon risiko (4)
1	Tidak ada transfer knowledge dari staf yang resign ke staf baru	Tinggi	Membuat regulasi prosedur resign
2	Belum ada portal internal untuk sharing info dan data proyek real time	Tinggi	Membangun portal untuk sharing info dan data proyek real time
3	Belum semua staf memiliki email internal dan masih menggunakan email pribadi menyebabkan lalu lintas data sulit dipantau	Tinggi	Setiap staf IT dibuatkan email internal
4	Keterlambatan staf dalam sharing info kebutuhan material	Tinggi	Menyediakan aplikasi khusus untuk mempercepat sharing info kebutuhan material
5	Data dari owner tidak lengkap	Tinggi	Membuat ceklist kelengkapan data yang masuk
6	Tidak ada pelatihan / training untuk meningkatkan skill staf	Tinggi	Memberi training secara rutin
7	Belum semua PC terhubung dan tersambung ke printer	Tinggi	Mengkonfigurasi jaringan agar semua perangkat terhubung
8	Skill staf masih kurang	Sedang	Memberi pelatihan yang diperlukan
9	Adanya informasi yang hilang saat ada staf resign	Sedang	Melakukan pencatatan rekapan pekerjaan setiap

No (1)	Uraian Risiko (2)	Kriteria Risiko (3)	Respon risiko (4)
	mendadak		hari
10	Spesifikasi hardware rendah	Sedang	Mengupgrade hardware
11	Penyimpanan data tidak teratur menyebabkan pencarian sulit	Sedang	Menyiapkan tempat khusus untuk menyimpan data proyek
12	Ada serangan malware	Sedang	Menyiapkan penangkal malware
13	Ada serangan virus	Sedang	Menyediakan anti virus
14	Staf merangkap tugas	Sedang	Menambah jumlah staf
15	Staf salah dalam membaca ukuran gambar	Sedang	Menambah SOP untuk melakukan cek ulang dalam membaca gambar
16	Kesalahan dalam menghitung kebutuhan material (BoQ)	Sedang	Menambah SOP untuk melakukan cek ulang setiap selesai perhitungan
17	Data hilang (tidak ada backup)	Sedang	Melakukan backup data rutin
18	Belum ada regulasi tertulis untuk penanganan masalah IT	Sedang	Dibuatkan standarisasi penanganan masalah IT
19	Jumlah SDM terbatas	Sedang	Rekrut karyawan baru
20	Belum ada aplikasi sebagai alat bantu untuk menghitung kebutuhan material	Sedang	Menyiapkan aplikasi sederhana untuk membantu perhitungan kebutuhan material
21	Belum ada perangkat keamanan TI	Sedang	Menyiapkan perangkat keamanan TI
22	Staf lalai dan menyebabkan kerusakan pada hardware	Rendah	Memberikan pengaman / perlindungan pada semua hardware
23	Software tidak update	Rendah	Mengupdate software
24	Software rusak	Rendah	Sedia software cadangan

Setelah pembuatan Tabel 4.10 di atas, selanjutnya diimplementasi atau dijalankan pada perusahaan XYZ sambil dilakukan pemantauan bagaimana

hasilnya setelah dilakukan penanganan. Pemantauan ini merupakan tahapan selanjutnya.

4.5 Pemantauan dan Pengendalian Risiko

Pada tahap ini dibuat tabel pengendalian risiko yang berisi tanggal dan status pengendalian (respon yang diberikan). Apakah sudah sesuai dengan yang direncanakan pada tahap sebelumnya atau belum. Berikut ini adalah Tabel 4.11 yang menunjukkan pengendalian risiko yang dibuat.

Tabel 4.11 Pengendalian Risiko

No	Risiko	Respon / Pengendalian	Tgl pengendalian	Status pengendalian			Saran perbaikan
				Baik	Cukup	Kurang	
1	Tidak ada transfer knowledge dari staf yang resign ke staf baru	Membuat regulasi prosedur resign	6 Juli 2017 (dalam perancangan)				
2	Belum ada portal internal untuk sharing info dan data proyek real time	Membangun portal untuk sharing info dan data proyek real time	6 Juli 2017 (dalam *requirement*)				
3	Belum semua staf memiliki email internal dan masih menggunakan email pribadi menyebabkan lalu lintas data sulit dipantau	Setiap staf IT dibuatkan email internal	6 Juli 2017 (dalam *requirement*)				
4	Keterlambatan staf dalam sharing info kebutuhan	Menyediakan aplikasi khusus untuk mempercepat	6 Juli 2017 (dalam *requirement*)				

No	Risiko	Respon / Pengendalian	Tgl pengendalian	Status pengendalian			Saran perbaikan
				Baik	Cukup	Kurang	
	material	sharing info kebutuhan material					
5	Data dari owner tidak lengkap	Membuat ceklist kelengkapan data yang masuk	6 Juli 2017	✓			
6	Tidak ada pelatihan / training untuk meningkatkan skill staf	Memberi training secara rutin					
7	Belum semua PC terhubung dan tersambung ke printer	Mengkonfigurasi jaringan agar semua perangkat terhubung	6 Juli 2017 (dalam progres)				
8	Skill staf masih kurang	Memberi pelatihan yang diperlukan					
9	Adanya informasi yang hilang saat ada staf resign mendadak	Melakukan pencatatan rekapan pekerjaan setiap hari					
10	Spesifikasi hardware rendah	Mengupgrade hardware	6 Juli 2017 (dalam progres)				
11	Penyimpanan data tidak teratur menyebabkan pencarian sulit	Menyiapkan tempat khusus untuk menyimpan data proyek	5 Juli 2017	✓			
12	Ada serangan malware	Menyiapkan penangkal	3 Juli 2017	✓			

No	Risiko	Respon / Pengendalian	Tgl pengendalian	Status pengendalian			Saran perbaikan
				Baik	Cukup	Kurang	
		malware					
13	Ada serangan virus	Menyediakan anti virus	3 Juli 2017	✓			
14	Staf merangkap tugas	Menambah jumlah staf					
15	Staf salah dalam membaca ukuran gambar	Menambah SOP untuk melakukan cek ulang dalam membaca gambar	4 Juli 2017	✓			
16	Kesalahan dalam menghitung kebutuhan material (BoQ)	Menambah SOP untuk melakukan cek ulang setiap selesai perhitungan	4 Juli 2017	✓			
17	Data hilang (tidak ada *backup*)	Melakukan *backup* data rutin	5 Juli 2017	✓			
18	Belum ada regulasi tertulis untuk penanganan masalah IT	Dibuatkan standarisasi penanganan masalah IT	4 Juli 2017 (dalam progres)				
19	Jumlah SDM terbatas	Rekrut karyawan baru					
20	Belum ada aplikasi sebagai alat bantu untuk menghitung kebutuhan material	Menyiapkan aplikasi sederhana untuk membantu perhitungan kebutuhan material					
21	Belum ada	Menyiapkan					

No	Risiko	Respon / Pengendalian	Tgl pengendalian	Status pengendalian			Saran perbaikan
				Baik	Cukup	Kurang	
	perangkat keamanan TI	perangkat keamanan TI					
22	Staf lalai dan menyebabkan kerusakan pada hardware	Memberikan pengaman / perlindungan pada semua hardware	23 Juni 2017	✓			
23	Software tidak update	Mengupdate software	4 Juli 2017		✓		
24	Software rusak	Sedia software cadangan	4 Juli 2017		✓		

Pada Tabel 4.11 diatas kolom tanggal, status, dan saran perbaikan belum bisa diisi karena belum terealisasi dikarenakan membutuhkan waktu yang lama. Tabel diatas bisa dipakai sebagai rencana untuk pelaksanaan pemantauan dan pengendalian risiko.

4.6 Komunikasi dan konsultasi.

Untuk pengkomunikasian risiko adalah dengan menyampaikan laporan *risk assessment* serta mengkomunikasikan risiko proses dan kebijakan manajemen risiko kepada seluruh personel yang berkaitan. Tahap ini sudah dicakup dalam tahap pemantauan dan pengendalian yang dilakukan berulang kali.

Setelah dilakukan proses percobaaan implementasi panduan manajemen risiko TI, selanjutnya diberikan kuesioner untuk mengevaluasi kemudahan penggunaan panduan kepada unit kerja IT. Hasil dari kuesioner kepada seluruh staf unit kerja IT yang berjumlah 4 orang seperti ditunjukkan pada Tabel 4.12 di bawah ini.

Tabel 4.12 Hasil kuesioner

Pertanyaan ke-	1	2	3	4	5	6	7	8
Jumlah pemilih SS			2	1				
Jumlah pemilih S	2	2	2	3	1	4	4	3
Jumlah pemilih N					2			1
Jumlah pemilih TS	2	2			1			

Jumlah pemilih ST								
Jumlah Total	4	4	4	4	4	4	4	4

Berdasar dari Tabel 4.12 di atas dapat diketahui bahwa dari hasil survei menunjukkan bahwa 50% responden setuju bahwa panduan manajemen risiko TI yang dibuat mudah dipahami dan dimengerti. Sedangkan 50% sisanya tidak setuju karena tidak terbiasa dan butuh waktu lama untuk memahaminya. Hal ini mengindikasikan panduan manajemen risiko TI cukup berpeluang untuk diterapkan di perusahaan melalui penerapan berulang hingga terbiasa. Dari pernyataan kedua, 50% responden setuju jika panduan mudah diikuti dan diterapkan. Sisanya sebanyak 50% tidak setuju dengan alasan belum paham dan membutuhkan penjelasan lebih lanjut untuk paham.

Dari pernyataan ketiga, 50% responden sangat setuju, dan 50% sisanya setuju bahwa panduan yang dibuat sangat bermanfaat dalam mengelola risiko. Hal ini menyiratkan bahwa panduan manajemen risiko TI yang dibuat bernilai manfaat dalam membantu keberlangsungan proyek dan perusahaan.

Dari pernyataan keempat, sebanyak 25% sangat setuju dan 75% sisanya setuju bahwa panduan tersebut masih memerlukan perbaikan. Saran yang diberikan untuk perbaikan antara lain panduan memerlukan penjelasan lebih detil untuk cara pengisian tabel-tabel, harapan untuk mengembangkan manajemen risiko, dan supaya ada pemberian waktu lebih lama untuk memahami tahapan manajemen risiko.

Dari pernyataan kelima, 25% setuju bahwa panduan yang dibuat sudah mencukupi kebutuhan perusahaan untuk mengelola risiko TI. Sedangkan 50% memilih netral, dan sisanya sebanyak 25% menjawab tidak setuju dengan alasan mungkin masih bisa digali lagi untuk identifikasi risiko, analisis dan penanganan risikonya.

Dari pernyataan keenam, 100% responden setuju bahwa panduan yang dibuat memudahkan dalam mengidentifikasi risiko TI. Dari pernyataan ketujuh, 100% responden setuju mendukung panduan manajemen risiko TI diterapkan secara reguler / periodik. Dari pernyataan kedelapan, 75% responden setuju

bahwa situasi pekerjaan / kantor memungkinkan untuk penerapan panduan tersebut secara rutin. Sedangkan 25% sisanya memilih netral.

Dari keseluruhan pernyataan dan hasil survei dapat diambil kesimpulan bahwa panduan manajemen risiko TI yang dibuat bermanfaat dan dapat diterapkan di perusahaan dengan disertai penjelasan yang lebih lengkap agar lebih mudah dipahami dan dimengerti.

halaman ini sengaja dikosongkan

BAB 5
KESIMPULAN DAN SARAN

Keberadaan manajemen risiko adalah suatu hal yang mutlak bagi perusahaan dan keberadaannya tidak bisa ditawar. Berikut ini kesimpulan dan saran dari penelitian ini.

5.1 Kesimpulan

Dari penelitian didapat beberapa kesimpulan sebagai berikut:

1. Melalui metode kombinasi COBIT, PMBOK dan ISO 31000 dapat menghasilkan panduan manajemen risiko TI yang bisa digunakan untuk mengelola risiko TI dan membantu kelancaran berjalannya proyek perusahaan XYZ.
2. Dari hasil identifikasi risiko diperoleh sebanyak 24 macam risiko TI yang berkaitan dengan proyek perusahaan.
3. Risiko yang telah teridentifikasi diketahui tingkatan atau level risiko IT. Dua macam risiko berada di tingkat rendah, tujuh belas macam risiko berada di tingkat sedang, dan lima macam risiko berada di tingkat tinggi. Belum ada risiko yang berada di tingkat ekstrim.
4. Dari hasil kuesioner terhadap staf IT diketahui bahwa panduan manajemen risiko TI yang dibuat dinilai bermanfaat dalam mendukung kelancaran proyek perusahaaan.

5.2 Saran

Adapun saran yang dapat diberikan pada penelitian ini agar bisa dijadikan rekomendasi untuk penelitian selanjutnya adalah sebagai berikut:

1. Panduan ini masih memerlukan perbaikan agar lebih mudah dipahami dan diterapkan.
2. Karena waktu yang terbatas, penelitian ini pada tahap pemantauan dan pengendalian risiko belum bisa diimplementasikan karena membutuhkan waktu yang tidak singkat.

3. Panduan ini diharapkan bisa diterapkan secara rutin dan diupdate terus saat ada risiko baru yang teridentifikasi.
4. Diharapkan nanti bisa dibuatkan manajemen risiko tidak terbatas di unit kerja IT saja.

DAFTAR PUSTAKA

Adelaide University, (2012), *Risk Management Handbook*, Life Impact, Group of Eight, The University of Adelaide, Australia: Adelaide.

Arief, Assaft, Hamsir, Iis., (2015), "An Integrative Framework of COBIT and TOGAF for Designing IT Governance in Local Government", *International Conference on Information Technology, Computer and Electrical Engineering*, Universitas Khairun, Ternate, hal. 36 – 39.

Bahsani, Samir., Semma, Alami., Sellam, Noura., (2015), "Towards a New Approach For Combining The IT Frameworks", *International Journal of Computer Science Issues* Vol. 12, No. 1, hal. 188 - 123.

Enslin, Z. (2012), "Cloud Computing Adoption: Control Objectives for Information and Related Technology (COBIT) - Mapped Risks and Risk Mitigating Controls", *African Journal of Business Management*, Vol. 6 No. 37, page 101854 – 10194.

Ernawati, Tati., Suhardi, R. Nugroho Doddi., (2012), "IT Risk Management Framework Based on ISO 31000:2009", *International Conference on System Engineering and Technology*, Institut Teknologi Bandung, hal. 99 – 106.

Flores, W., Sommestad, T., Holm, H., Ekstedt, M. (2011), "Assessing Future Value of Investments in Security – Related IT Governance Control", *Electronic Journal of Information Systems Evaluation*, Vol. 14, hal. 216 – 227.

Indah, Dwi Rosa., Harlili, Firdaus Arfiyan. (2014), "Risk Management for ERP Post Implementation Using Cobit 5 for Risk", *Proceeding of the 1st International Conference on Computer and Science Engineering*, Eds: Beckhoum, Kamal, et al, Universitas Sriwijaya, Palembang, hal. 113 - 118.

International Standard for Organization, (2009), *Risk Management - Principles and Guidelines*, International Standard for Organization, Geneva Switzerland.

Isaca, (2013), *A Business Framework for the Governance and Management of Enterprise IT*, Isaca, USA.

Isaca, (2013), *COBIT 5 for Risk*, Isaca, USA.

Lark, John. (2015), *ISO 31000: Risk Management – A Practical guide for SMEs*, ISO, Geneva Switzerland.

Marcelino, Sara., Villanueva, Pedro. (2013), "Project risk management methodology for small firms", *International Journal of Project Management* Vol. 32, hal. 327 – 340.

Parent, M., Reich, B. H. (2009), *Governing Information Technology Risk*, Vol. 51, Barkeley University, California.

Project Management Institute, (2013), *A Guide to the Project Management Body of Knowledge – Fifth Edition*, Project Management Institute, Inc, Pennsylvania.

Rahmadhanty, Dwiani. (2010), *Penerapan Tata Kelola Teknologi Informasi dengan Menggunakan COBIT Framework 4.1 (Studi Kasus pada PT. Indonesia Power)*, Tesis, Universitas Indonesia, Jakarta.

Tanuwijaya, H. dan Sarno, R. (2010), "Comparation of COBIT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals", *International Journal of Computer Science and Network Security*, Vol.10 No.6, Surabaya.

LAMPIRAN

Wawancara 1:

Tujuan : Memperoleh informasi mengenai kondisi perlakuan risiko pada perusahaan XYZ

Waktu : Selasa, 7 Maret 2017

Lokasi : Kantor perusahaan XYZ

Narasumber : Adi Wijaya

Jabatan : Direktur

Pertanyaan

1. Bagaimana manajemen / pengelolaan risiko di perusahaan XYZ?
   Selama ini memang perusahaan belum memiliki standar atau prosedur untuk pengelolaan risiko terutama pada proyek.
2. Seperti apa bentuk pengelolaan risiko yang ada sekarang?
   Jika ada peristiwa tidak terduga biasanya direspon secara spontan dan ditangani berdasar kebiasaan.
3. Apakah terdapat prosedur khusus dalam menangani risiko?
   Tidak / belum ada.
4. Apakah teknologi informasi berperan penting terhadap keberlangsungan proyek?
   Ya, peran teknologi informasi cukup penting bagi keberlangsungan dan kelancaran proyek. Karena semua informasi banyak bersumber dan diolah disana.
5. Ketika terjadi risiko pada aktivitas teknologi informasi apakah cukup berdampak pada kelancaran proyek?
   Dampaknya sangat terasa bagi kelancaran proyek, karena kegagalan pada proses IT bisa membuat proyek rugi materi dan waktu

Wawancara 2:

Tujuan :

Waktu : Selasa, 7 Maret 2017

Lokasi : Kantor perusahaan XYZ

Narasumber : Eko Nopi S

Jabatan : Supervisor unit kerja IT

Pertanyaan

1. Apa saja perisitiwa TI yang berisiko terhadap keberlangsungan proyek?
   Kecepatan arus informasi, ketepatan perhitungan kebutuhan material (BoQ), kelancaran data teknis, keamanan data, dan transfer knowledge.
2. Dari peristiwa tersebut manakah yang paling sering muncul saat berlangsungnya proyek?
   Kesemuanya cukup sering muncul saat proyek sedang berjalan dan jika terjadi cukup mengganggu kelancaran proyek.
3. Peristiwa apa yang memiliki dampak paling besar terhadap keberhasilan proyek?
   Sejauh ini yang dampaknya besar adalah kesalahan dalam menghitung kebutuhan material yang diperlukan untuk proyek. Itu adalah kesalahan yang tidak bisa ditolerir oleh pemilik perusahaan karena berdampak langsung pada keuntungan dan merugikan perusahaan.
4. Apakah sudah ada pengkategorisasian risiko?
   Belum ada.
5. Apakah ada pencatatan terhadap risiko-risiko yang pernah terjadi?
   Selama ini belum ada pencatatan khusus mengenai risiko-risiko yang pernah terjadi.

Kuesioner penggunaan panduan manajemen risiko TI

Tujuan : Mengevaluasi kemudahan penggunaan panduan manajemen risiko TI

Waktu : Jumat, 23 Juni 2017

Lokasi : Kantor Perusahaan XYZ

Nama :

Jabatan:

Petunjuk

Dari pernyataan berikut ini manakah yang paling sesuai menurut Anda? Nyatakan dengan:

SS : Sangat Setuju

S : Setuju

N : Netral

TS : Tidak Setuju

ST : Sangat Tidak Setuju

No	Pernyataan	SS	S	N	TS	ST
1	Panduan ini mudah dipahami dan dimengerti					
2	Panduan ini mudah diikuti dan diterapkan dalam pengelolaan risiko					
3	Panduan ini sangat bermanfaat dalam mengelola risiko					
4	Panduan ini masih memerlukan perbaikan					
5	Panduan ini sudah mencukupi kebutuhan perusahaan untuk mengelola risiko TI					
6	Panduan ini memudahkan dalam mengidentifikasi risiko TI					

7	Saya mendukung panduan ini diterapkan secara reguler / periodik					
8	Situasi pekerjaan / kantor memungkinkan untuk penerapan panduan ini secara rutin					

Pertanyaan:

1. Jika Anda menjawab tidak setuju pada pernyataan no. 1 sebutkan alasannya!

Jawaban : ……..

2. Jika Anda menjawab tidak setuju pada pernyataan no. 2 sebutkan alasannya!

Jawaban : ……..

3. Jika Anda menjawab tidak setuju pada pernyataan no. 3 sebutkan alasannya!

Jawaban : ……..

4. Jika Anda menjawab setuju pada pernyataan no. 4 maka berikan saran untuk perbaikan panduan yang telah dibuat, dan bila memilih tidak setuju sebutkan alasannya!

Jawaban : ……..

5. Jika Anda menjawab tidak setuju pada pernyataan no. 5 sebutkan alasannya!

Jawaban : ……..

6. Jika Anda menjawab tidak setuju pada pernyataan no. 6 sebutkan alasannya!

Jawaban : ……..

7. Jika Anda menjawab tidak setuju pada pernyataan no. 7 sebutkan alasannya!

Jawaban : ……..

8. Jika Anda menjawab tidak setuju pada pernyataan no. 8 sebutkan alasannya!

Jawaban : ……..

Panduan Manajemen Risiko TI pada proyek Perusahaan XYZ

Manajemen risiko IT merupakan serangkaian proses untuk mengelola risiko terkait IT yang berhubungan dengan keberlangsungan proyek perusahaan. Prosesnya meliputi perencanaan, identifikasi, analisis, respon (penanganan), pemantauan dan pengendalian serta pengkomunikasian risiko dari setiap aktivitas IT yang dilaksanakan oleh perusahaan. Dalam upaya mewujudkan kelancaran proyek yang dijalankan oleh perusahaan, maka divisi / unit kerja IT perlu menerapkan manajemen risiko sebagai sistem peringatan dini (*early warning system*) dan untuk mendukung penuh keberhasilan proyek yang sedang ditangani oleh perusahaan. Pelaku yang terlibat dalam pembuatan dan pengecekan dokumen adalah direksi, manajemen, dan unit kerja/divisi IT.

1. Perencanaan Manajemen Risiko

Pada tahap ini dasar yang dipakai adalah dari PMBOK dan ISO 310000. Berdasar PMBOK tahap perencanaan manajemen risiko berisi rencana dasar untuk menghadapi risiko. Yang dijadikan input atau landasan/pijakan pada tahap ini adalah rencana manajemen proyek, kontrak/perjanjian pekerjaan, kondisi lingkungan perusahaan, dan proses organisasi. Dimana outputnya adalah berupa rencana manajemen risiko. Hal ini bisa dilakukan melalui rapat perencanaan dan analisis. Template berupa tabel untuk mendefinisikan level risiko, kemungkinan (*probability*), dampak (*impact*), dan matrik perkalian *probability* dan *impact* dibuat untuk diisikan nanti pada tahap analisis risiko.

Tabel Ukuran Kemungkinan

Level	Probabilitas	Kriteria
1	Jarang	Probabilitas kejadian ≤ 20%
2	Kemungkinan kecil	Probabilitas kejadian 20% < x ≤ 40%
3	Kemungkinan sedang	Probabilitas kejadian 40% < x ≤ 60%
4	Kemungkinan besar	Probabilitas kejadian 60% < x ≤ 80%
5	Hampir pasti	Probabilitas kejadian 80% < x ≤ 100%

Di atas adalah tabel ukuran kemungkinan untuk menentukan standar ukuran dari probabilitas kejadian dari risiko TI.

Tabel Ukuran Dampak

Level	Dampak	Uraian
1	Tidak signifikan	Dampaknya dapat ditangani dan tidak mempengaruhi kelancaran proyek
2	Kecil	Sedikit mempengaruhi kelancaran proyek
3	Sedang	Mengganggu kelancaran proyek
4	Besar	Kerugian cukup besar terhadap keberlangsungan proyek dan perusahaan
5	Luar biasa	Menimbulkan bencana/kerugian yang sangat besar pada proyek

Di atas adalah tabel ukuran dampak untuk menentukan standar dampak dari akibat timbulnya risiko TI yang terjadi.

Kemudian berdasar ISO 31000 tahap perencanaan manajemen risiko disejajarkan dengan penetapan ruang lingkup. Dimana pada ISO 31000 tahap ini terdiri dari empat aktivitas yaitu, penetapan ruang lingkup internal, penetapan ruang lingkup eksternal, penetapan ruang lingkup proses manajemen risiko, dan membangun kriteria risiko. Jadi, yang perlu dilakukan pada tahap ini adalah sebagai berikut :

1. Membuat rencana manajemen risiko proyek yang memuat metodologi, peran dan tanggung jawab, keuangan, jadwal, kategori risiko, definisi kemungkinan dan dampak dari risiko, matriks kemungkinan dan dampak risiko, penetapan *risk appetite* dan *risk tolerance* dari stakeholder, laporan, serta *tracking*.

   Tabel Penetapan *Risk Appetite* dan *Risk Tolerance*

Risk Appetite	…… …… ……
Risk Tolerance	…… …… ……

   Tanggal pengisian:

2. Menetapkan ruang lingkup manajemen risiko yang meliputi internal, eksternal, proses manajemen risiko, dan mengembangkan kriteria risiko.

2. Identifikasi Risiko

Identifikasi risiko ini mengacu pada COBIT tahap pengumpulan data. Yang perlu dilakukan pada tahap ini adalah membuat *risk scenario*. Contoh tabelnya sebagai berikut:

Tabel *Risk scenario*

No	Jenis Risiko	Tipe Risiko			Skenario Risiko	
		IT benefit / value enablement risk	*IT programme and project delivery risk*	*IT operations and service delivery risk*	Skenario Negatif	Skenario Positif

Tanggal pengisian:

Nama Anggota Penyusun:

(Direktur) Paraf setuju	(Manajer) Paraf setuju

COBIT membagi tipe risiko menjadi tiga, yaitu sebagai berikut:

a. *IT benefit / value enablement risk*, dimana risiko yang diidentifikasi masuk ke dalam tipe manfaat atau nilai risiko TI, yaitu apabila risiko terkait dengan (kehilangan) kesempatan untuk memanfaatkan TI dalam meningkatkan efisiensi atau efektivitas proses bisnis atau sebagai enabler untuk inisiatif bisnis baru.

Contohnya adalah teknologi yang digunakan dalam inisiatif bisnis baru dan teknologi yang digunakan untuk mengefisiensikan proses operasional.

b. *IT programme and project delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam tipe program dan proyek risiko TI, yaitu apabila risiko terkait dengan kontribusi TI untuk membuatkan atau meningkatkan solusi bisnis, biasanya dalam bentuk proyek dan program. Contohnya adalah kualitas proyek, relevansi proyek dan kelebihan waktu proyek dari yang ditentukan.
c. *IT operations and service delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam tipe operasional dan layanan risiko TI, yaitu apabila risiko terkait dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan TI, dimana risiko dapat membawa kerugian atau pengurangan nilai perusahaan. Contohnya adalah gangguan pada layanan TI, masalah keamanan dan isu-isu terkait.

IT benefit / value enablement risk, diisi dengan ‘P’ (Primer) apabila risiko terkait TI sebagai enabler untuk meningkatkan solusi binis, sedangkan jika tidak terkait maka diisi dengan ‘S’.
IT programme and project delivery risk, diisi dengan ‘P’ (Primer) apabila risiko terkait dengan program dan proyek TI, sedangkan jika tidak terkait maka diisi dengan ‘S’.
IT operations and service delivery risk, diisi dengan ‘P’ (Primer) apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, sedangkan jika tidak terkait maka diisi dengan ‘S’.

Mengacu kepada standar COBIT 5 for Risks, terdapat dua puluh jenis (kategori) risiko TI untuk setiap risiko yang diidentifikasi, berikut merupakan pembagian dua puluh jenis risiko tersebut yang disajikan pada Tabel berikut:

Tabel Pembagian Jenis (Kategori) Risiko

No	Kategori	Pengertian
1	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio
2	*Programme/ projects life cycle management (programme/ project initiation, economics, delivery, quality and termination)*	Manajemen siklus hidup program atau proyek (inisiasi program/proyek, biaya, delivery, kualitas dan penutupan proyek)
3	*IT investment decision making*	Pengambilan keputusan investasi TI
4	*IT expertise and skills*	Ketrampilan dan keahlian TI
5	*Staff operations (human error and malicious intent)*	Staff operasional (kesalahan faktor manusia disengaja maupun tidak)
6	*Information (data breach: damage, leakage and access)*	Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)
7	*Architectural (vision and design)*	Arsitektur (visi dan desain)
8	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*	Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)
9	*Software*	Perangkat lunak
10	*Business ownership of IT*	Kepemilikan bisnis TI
11	*Supplier selection/performanse, contractual compliance, termination of service and transfer*	Pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan
12	*Regulatory compliance*	Pemenuhan regulasi
13	*Geopolitical*	Geopolitik
14	*Insfrastructure theft or destruction*	Pencurian infrastruktur atau pengrusakan
15	*Malware*	Malware
16	*Logical attacks*	Serangan langsung pada sistem, perangkat lunak, ataupun data
17	*Industrial action*	Situasi dalam dunia industri
18	*Environmental*	Lingkungan
19	*Acts of Nature*	Bencana alam
20	*Innovation*	Inovasi

3. Analisis Risiko

Analisis kualitatif dibuat untuk memberikan gambaran umum tentang level risiko. Analisis kualitatif menggunakan bentuk kata atau skala deskriptif untuk menjelaskan seberapa besar potensi risiko yang diukur. Apakah termasuk level risiko rendah, sedang, atau tinggi.

Setelah itu dapat dilakukan analisis semi kuantitatif ataupun kuantitatif untuk lebih merinci level risiko yang ada.

Pada analisis semi kuantitatif, skala kualitatif yang telah disebutkan diatas diberi nilai yang menggambarkan besaran kemungkinan maupun dampak risiko. Hasilnya berupa tingkat risiko yang merupakan perkalian dari keduanya.

Pada analisis kuantitatif yang digunakan adalah nilai numerik. Probabilitas/frekuensi kejadian beserta dampaknya dituangkan dalam bentuk numerik untuk menentukan tingkatan risikonya.

Tabel Risk Map

Dampak / Kemungkinan	1 Sangat kecil	2 Kecil	3 Biasa	4 Besar	5 Luar biasa
5 Sering terjadi	5 Sedang	10 Sedang	15 Tinggi	20 Ekstrim	25 Ekstrim
4 Sering	4 Rendah	8 Sedang	12 Tinggi	16 Tinggi	20 Ekstrim
3 Biasa	3 Rendah	6 Sedang	9 Sedang	12 Tinggi	15 Tinggi
2 Jarang	2 Rendah	4 Rendah	6 Sedang	8 Sedang	10 Tinggi
1 Sangat jarang	1 Rendah	2 Rendah	3 Rendah	4 Rendah	5 Sedang

Di atas adalah tabel *Risk Map* untuk menentukan tingkat risiko berdasar kemungkinan yang dikalikan dengan dampak yang ditimbulkan.

Tabel Kriteria Risiko

Level Risiko	Kriteria	Uraian
Rendah	Dapat diterima dan dilakukan pemantauan	Dibutuhkan pengendalian normal
Sedang	Perlu pengendalian risiko	Dibutuhkan pengendalian yang baik
Tinggi	Perlu pengendalian yang ketat	Dibutuhkan pengendalian yang sangat baik (*excellent*)
Ekstrim	Tidak dapat diterima	Dibutuhkan pengendalian yang sangat baik (*excellent*)

Di atas adalah tabel kriteria risiko yang dipakai sebagai standar untuk merencanakan respon risiko yang akan dipilih.

4. Perencanaan Penanganan Risiko

Untuk menentukan respon terhadap risiko bisa digunakan metode estimasi/perkiraan secara subyektif. Metode ini disebut *professional judgement* (*Control Self-Assessment Techniques/ CST*). Pemilihan respon terhadap risiko berdasarkan alternatif yang tersedia (*accept, mitigate, transfer, avoid*) untuk risiko negatif, dan untuk risiko positif tersedia *exploit*, *enhance*, *share*, dan *ignore*.

Tabel R*isk Response*

No (1)	Uraian Risiko (2)	Kriteria risiko (3)	Kemungkinan (4)	Dampak (5)	Kemungkinan x Dampak (6)	Respon risiko (7)

Tanggal penyusunan:

(Direktur) Paraf setuju	(Manajer) Paraf setuju

Petunjuk pengisian berdasar kolom yang ada:

(1) Diisi nomor urut

(2) Diisi mengenai gambaran risiko yang ada

(3) Diisi kriteria risikonya

(4) Diisi dengan skala linkert (1 - 5) yang menunjukkan ukuran kemungkinan terjadinya risiko

(5) Diisi dengan skala linkert (1 - 5) yang menunjukkan ukuran dampak risiko

(6) Diisi dengan hasil perkalian kolom (4) dan (5)

(7) Diisi respon risiko yang dipilih

5. Pemantauan dan Pengendalian Risiko

Tabel Pengendalian Risiko

No	Risiko	Pengendalian	Tgl pengendalian	Status pengendalian			Saran perbaikan
				Baik	Cukup	Kurang	

Tanggal pengisian:

Nama Anggota Penyusun:

(Direktur) Paraf setuju	(Manajer) Paraf setuju

Di atas adalah tabel pengendalian risiko untuk memantau dan melihat status pengendalian dari risiko TI serta saran yang diusulkan sebagai perbaikan.

6. Untuk pengkomunikasian risiko adalah dengan menyampaikan laporan *risk assessment* serta mengkomunikasikan risiko proses dan kebijakan manajemen risiko kepada seluruh personel yang berkaitan.

Hasil Kuesioner penggunaan panduan manajemen risiko TI

Waktu : Jumat, 23 Juni 2017

Lokasi : Kantor Perusahaan XYZ

Nama Responden : 1. Eko Nopi S

2. Hurin Iin

3. Masrohan

4. Luzi Aprillia

Pernyataan 1	Jawaban				
	SS	S	N	TS	ST
Panduan ini mudah dipahami dan dimengerti		2		2	
Total Jawaban		**2**		**2**	

Pernyataan 2	Jawaban				
	SS	S	N	TS	ST
Panduan ini mudah diikuti dan diterapkan dalam pengelolaan risiko		2		2	
Total Jawaban		**2**		**2**	

Pernyataan 3	Jawaban				
	SS	S	N	TS	ST
Panduan ini sangat bermanfaat dalam mengelola risiko	2	2			
Total Jawaban	**2**	**2**			

Pernyataan 4	Jawaban				
	SS	S	N	TS	ST
Panduan ini masih memerlukan perbaikan	1	3			
Total Jawaban	**1**	**3**			

Pernyataan 5	Jawaban				
	SS	S	N	TS	ST
Panduan ini sudah mencukupi kebutuhan perusahaan untuk mengelola risiko TI		1	2	1	
Total Jawaban		**1**	**2**	**1**	

Pernyataan 6	Jawaban				
	SS	S	N	TS	ST
Panduan ini memudahkan dalam mengidentifikasi risiko TI		4			
Total Jawaban		**4**			

Pernyataan 7	Jawaban				
	SS	S	N	TS	ST
Saya mendukung panduan ini diterapkan secara reguler / periodik		4			
Total Jawaban		**4**			

Pernyataan 8	Jawaban				
	SS	S	N	TS	ST
Situasi pekerjaan / kantor memungkinkan untuk penerapan panduan ini secara rutin		3	1		
Total Jawaban		**3**	**1**		

BIOGRAFI PENULIS

Hurin Iin, S.ST adalah putri pertama dari tiga bersaudara. Lahir di Jombang, 7 Desember 1986. Menempuh pendidikan MIN Darul Ulum Rejoso, SLTP Negeri 1 Peterongan, dan Lulus SMAN 2 Jombang pada tahun 2005, dan melanjutkan studi Diploma IV (D4) di Teknik Informatika, Politeknik Elektronika Negeri Surabaya (PENS), hingga lulus pada tahun 2009. Dalam studi D4-nya di Teknik Informatika, Politeknik Elektronika Negeri Surabaya penulis sempat bekerja dan melanjutkan studi S2-nya di MMT-ITS.

Penulis bisa dihubungi melalui email huriniin@gmail.com.